AutoCrypt V2X PKI Root CA

Certificate Practices Statement

(Root CA CPS)

V1.0

2026.02.06

<Enactment / Amendment History>

Version	Category	Name	Date
V1.0	Enacted	Jaewoo Kim	2026/02/06

Table of Contents

1. Introduction

1.1. Overview

This document serves as the Certification Practices Statement (CPS) for AutoCrypt Co., Ltd. ("AutoCrypt"), describing the principles, practices, and procedures governing AutoCrypt's V2X security certification services. This CPS applies to all entities that participate in or rely upon AutoCrypt's certification services, including vehicles, roadside infrastructure, and V2X-related certification system organizations within a secure autonomous and cooperative driving environment.

As part of AutoCrypt's certification framework, this CPS establishes the technical, legal, and business requirements for the issuance, distribution, management, and revocation of digital certificates. AutoCrypt operates as the Root Certification Authority (Root CA) within this framework, enabling subordinate certification authorities to perform their certification functions in accordance with defined policies and procedures.

This CPS is structured in accordance with the framework of RFC 3647 and is designed based on the Security Credential Management System (SCMS) architecture. It follows the technical standards specified in IEEE 1609.2.1. All V2X certificates issued by AutoCrypt conform to the IEEE 1609.2.1 certificate format, unless otherwise specified (e.g., X.509 for Enrollment Certificates).

1.2. Document name and identification

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

1.3. PKI participants

1.3.1. SCMS Manager

The SCMS Manager is a security policy and standards body composed of organizations with a vested interest in the long-term successful operation of the US V2X ecosystem (including automotive OEMs; providers of vehicle, roadside infrastructure, and traffic management technologies, products, and services; and federal, state, and local transportation and safety agencies).

To maintain the security and reliability of the V2X ecosystem, the SCMS Manager establishes, publishes, and maintains interoperability profiles, policies, procedures, and guidelines, and conducts related R&D.

The SCMS Manager oversees the overall system comprising Electors, Root CAs, SCMS components, and End Entities (vehicle OBUs, RSUs, etc.), and continuously monitors compliance with SCMS Manager best practices and policies through participant audits. It annually verifies that organizations contracted with the SCMS Manager, such as Root CAs and Electors, are complying with ecosystem standards, policies, guidelines, and contractual obligations. If a non-compliant organization is identified, the SCMS Manager performs the role of recommending the removal or revocation of that organization from the V2X ecosystem under its supervision.

1.3.2. Electors

Electors are entities authorized to approve and sign the Certificate Trust List (CTL).

1.3.3. Accredited PKI Auditor

The Accredited PKI Auditor shall be an independent third-party organization accredited to audit SCMS Providers in accordance with the requirements set forth in Section 8 of this Certificate Policy.

The responsibilities of the Accredited PKI Auditor shall include the following:

1. Auditing the SCMS Provider that operates a Root CA and any applicable Subordinate Certification Authorities (Sub-CAs);

2. Receiving and reviewing the applicable Certification Practice Statement (CPS) of the SCMS Provider;

3. Delivering the audit results to the appropriate trust authority or governing body for validation of the SCMS Provider's Root CA trust status;

4. Determining whether modifications to the Certificate Policy (CP) or CPS require a supplementary audit;

5. Being accredited to audit End Entity devices, where applicable, in accordance with the Certificate Policy.

1.3.4. SCMS Provider

The SCMS Provider operates one or more SCMS model elements in accordance with IEEE 1609.2.1, including the Root CA, Intermediate CA (ICA), Enrollment CA (ECA), Authorization CA (ACA), Registration Authority (RA), Linkage Authority (LA), Misbehavior Authority (MA), and CRL Signer.

The SCMS Provider shall provide Public Key Infrastructure (PKI) services necessary for the issuance, management, validation, and revocation status checking of certificates within the V2X ecosystem.

Each SCMS Provider shall maintain one or more Certification Practice Statements (CPS) that fully comply with the applicable SCMS Certificate Policy (CP), and all SCMS services and Certification Authorities (CAs) shall be operated in accordance with the approved CPS.

The SCMS Provider shall be subject to regular compliance audits against the SCMS CP and its CPS, and shall apply for inclusion of its Root CA certificate in the Certificate Trust List (CTL) as part of the trust establishment process. In addition, the SCMS Provider shall submit periodic audit results to the SCMS Manager in accordance with the audit frequency defined in the applicable audit requirements.

1.3.4.1 Root CA

This Certification Practices Statement (CPS) applies solely to the AutoCrypt V2X Root Certification Authority (Root CA).

Certification practices associated with any subordinate certification authorities within the CA hierarchy, including Enrollment CAs (ECA) and Authorization CAs (ACA), where applicable, shall be documented in one or more separate CPS documents.

The AutoCrypt V2X Root CA forms part of the certification path used to issue certificates under the AutoCrypt V2X trust domain. This trust domain may be operated as part of a broader SCMS-based V2X trust framework.

All certification practices of the AutoCrypt V2X Root CA comply with the applicable SCMS Certificate Policy.

The Root CA certificate profiles are consistent with the certificate profiles specified in IEEE 1609.2 and IEEE 1609.2.1.

The AutoCrypt V2X Root CA is the top-level certification authority that issues certificates to subordinate CAs and is self-signed. Due to the critical security impact of a Root CA compromise, the AutoCrypt V2X Root CA is maintained under strict security controls and is brought online only when operationally necessary.

1.3.4.2 Intermediate CA (ICA)

A CA whose certificate was issued by another CA and whose main responsibility is to issue certificates to other CAs, like ACA and ECA.

1.3.4.3 Enrollment CA(ECA)

A CA whose main responsibility is to issue enrollment certificates.

The initial enrollment certificate shall be provisioned via DCM or ECA, while the successor enrollment certificate shall be provisioned by the RA.

Enrollment CA shall support IEEE 1609.2.1 enrollment certificates for enrollment certificate request.

1.3.4.4 Authorization CA(ACA)

A CA whose main responsibility is to issue authorization certificates.

1.3.4.5 CRL Signer

A CAs CRL can be signed by the CA itself or alternatively by a CRL Signer.

1.3.4.6 Distribution Center

AutoCrypt have a Distribution Center, where the following public information shall be available, if applicable:

https://dc.v2x.autocrypt.io

1. Certificates included in the chain (Root CA, ICA, ECA, ACA),
2. Certificate Chain File(CCF),
3. Certificate Revocation Lists(CRLs),
4. composite CRL, including CTL according to IEEE 1609.2.1.,
5. Certificate Trust Lists(CTLs),
6. CRLs for all CRACA according to IEEE 1609.2.1., if CRL Signer is used.

1.3.4.7 Linkage Authority (LA)

A component of the Security Credential Management System (SCMS) that provides inputs to the linkage value

calculation process to enable efficient revocation (large number in one step) of pseudonym certificates while preserving the privacy of an End Entity (EE) against the Authorization Certificate Authority (ACA).

1.3.4.8 Misbehavior Authority (MA)

A component of the Security Credential Management System (SCMS) that receives reports of malicious or potentially malicious application activities, analyzes them, and determines whether or not to take mitigating actions. MA operates in cooperation with LA, RA and ACA.

A MA should cooperate with all SCMS Providers published on the CTL.

A MA should provide linking information for reported ACAs.

A MA should support the end entity revocation requests from other MAs.

1.3.4.9 Registration Authority (RA)

A component of the Security Credential Management System (SCMS) that is generally the main point of contact for an End Entity (EE) and is responsible for provisioning the EE with authorization and successor enrollment certificates. RA also provides system information.

The tasks of an RA are the following:

1. Supporting the authorization certificate provision to valid end entities,

2. Supporting the successor enrollment certificate provision to valid end entities,

3. Providing system information for end entities (CTL, Certificate chain certificates, CRL, CCF)

4. Forwards misbehavior reports for MA.

1.3.4.10 Device Configuration Manager(DCM)

An optional component of the SCMS that is responsible for bootstrapping an EE and providing secure connection between the EE and the ECA.

1.4. Certificate usage

1.4.1. Applicable domains of use

Certificates issued under the present CPS are intended to be used to validate digital signatures and encryption/decryption in the SCMS V2X communication context.

Certificates are issued in accordance with the SCMS Manager Certificate Policy based on the SCMS reference architecture and IEEE 1609.2 and IEEE1609.2.1 specifications. The certificate profiles defined in IEEE 1609.2.1 determine the certificate usages of the SCMS ecosystem entities.

1.4.2. Limits of responsibility

Certificates are not intended, nor authorized, for use in:

1. circumstances that offend, breach or contravene any applicable law, regulation, decree or government order,

2. circumstances that breach, contravene or infringe the rights of others,

3. breach of this CP or the relevant subscriber agreement,

4. any circumstances where their use could lead directly to death, personal injury or severe environmental damage (e.g. through failure in the operation of nuclear facilities, aircraft navigation or communication, or weapons control systems),

5. circumstances that contravene the overall objectives of greater road safety and more efficient road transport in North America, Australia, Korea, Japan or another jurisdiction.

1.5. Policy administration

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

- Department: AutoCrypt V2X PKI Root CA Security Certification Center
- Phone Number: +82-2-2125-4000
- Address: (07241) 6F Sewoo Building, 115 Yeouigongwon-ro, Yeongdeungpo-gu, Seoul, South Korea
- E-mail: rootca@autocrypt.io

1.5.1. Updating of this CPS

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

- Approval of current and future versions of CPS
- 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. CPS approval procedures

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.
- Prior to the commencement of services (point-in-time audit), and during each periodic compliance re-evaluation, AutoCrypt shall submit its CPS to an accredited independent PKI auditor as part of the formal compliance audit process.
- The established and revised Certification Practices Statement shall be implemented from the date of report.

1.6. Definitions and acronyms

The definitions and acronyms of IEEE 1609.2.1-2022 (Section 3.1 and 3.2) apply.

For easy reading, they are referenced below:

Application Activities: The activities that are carried out to achieve the business or operational goals of a distributed application.

Application Domain: The collection of application instances and management services that carry out and support a specific collection of application activities.

Application Instance: A single instance of an implementation of a component of a distributed application, running on a single device (or perceived as running on a single device from the perspective of other participants in the application domain).

Authorization Certificate: A certificate that is used to authorize application activities. Contrast: enrollment certificate.

Authorization Certificate Authority (ACA): A Certificate Authority (CA) whose main responsibility is to issue authorization certificates.

Binary Hash Tree: A data structure in which each node at level l + 1 has its value derived by applying a hash function to its parent node at level l, such that the publication of one node value at level l + 1 allows the derivation of all node values at levels l and below.

Blocked Enrollment Certificate: An enrollment certificate that has been determined to be no longer eligible to authorize certificate requests or certificate download requests.

Butterfly Key: The final cryptographic public key or private key produced by the butterfly key process.

Butterfly Key Certificate Request: A request created by an End Entity that is intended to result in the issuance of multiple certificates, with the keys in those certificates created via the butterfly key process.

Butterfly Key Expander (BKE): A component of the Security Credential Management System that adds an additional random elliptic curve point to each cocoon public key to create the butterfly public key (or the implicit certificate) for an explicit certificate.

Butterfly Key Parameters: The caterpillar public key and the expansion function used in the butterfly key process.

Butterfly Key Process: A process used in certificate generation where an initial caterpillar public key is modified using an expansion function by the Cocoon Key Expander (CKE) to create a cocoon public key, and further modified by a BKE to produce a butterfly public key (or an implicit certificate) for an explicit certificate, in such a way that only the holder of the original caterpillar private key can derive the butterfly private key corresponding to the butterfly public key (or, the implicit certificate). It is infeasible for a party that does not know the caterpillar private key to derive the corresponding butterfly private key.

Butterfly Public Key: The final cryptographic public key produced by the butterfly key process.

Canonical Identifier: A device identifier used to look up the device's canonical key.

Canonical Key: A device key with a long lifetime, used to request enrollment certificates.

Canonical key acceptance policy: A set of conditions applied to a canonical key and its metadata to determine whether that key is acceptable to authorize an enrollment certificate request received by a particular Enrollment Certificate Authority (ECA).

Caterpillar Key: The initial cryptographic public key or private key input to the butterfly key process.

Caterpillar Private Key: The initial cryptographic private key input to the butterfly key process.

Caterpillar Public Key: The initial cryptographic public key input to the butterfly key process.

Certificate Acceptance Policy: A policy setting constraints on the digital certificates (ITU-T Recommendation X.509 or IEEE Std 1609.2 based) that may be used to authorize certain activities.

Certificate Acceptance Policy: A statement of properties that a SCMS component certificate is required to have when it is used to authenticate that SCMS component in the context of a Transport Layer Security (TLS) session.

Certificate Trust List (CTL): A list of the Electors and the root certificate authorities (Root CAs) that are trusted by a particular SCMS Manager, signed by the eligible Electors.

Characterization Parameters: Parameters used to indicate properties of a protocol mechanism (secure session or Web API) specified in this document, with the purpose of making the properties of a composite protocol (secure session + Web API) clear.

Client (of a registration authority [RA]): Any entity within the system that uses a particular Registration Authority (RA) for certificate management activities.

Cocoon Key Expander (CKE): A component of the SCMS that uses the expansion function to create a series of statistically uncorrelated cocoon public keys.

Cocoon Key: The intermediate cryptographic public key or private key produced by applying an expansion function to a caterpillar key in the butterfly key process.

Cocoon Private Key: The intermediate cryptographic private key produced by applying an expansion function to a caterpillar private key in the butterfly key process.

Cocoon Public Key: The intermediate cryptographic public key produced by applying an expansion function to a caterpillar public key in the butterfly key process.

Delegated Registration Authority: An organization responsible for assigning identifiers, or identifier sets, from a designated range of values of the identifier CtlSeriesId defined in this standard. The name indicates that the authority to assign from the indicated range has been assigned to the delegated registration authority by the

IEEE Registration Authority.

Derivable Node: A node in a binary hash tree whose value can be derived from published node values.

Device Configuration Manager (DCM): A component of the SCMS that is responsible for bootstrapping an End Entity and providing secure connection between the EE and the Enrollment Certificate Authority (ECA).

Direct Authorization (for enrollment certificate request): A mode of authorization for enrollment certificate request where the enrollment certificate request generated by an EE device contains a proof that the device is entitled to that enrollment certificate.

Direct Communication: communication between road user and the infrastructure directly. (for example PC5).

Distribution Center (DC): A component of the SCMS that distributes public information such as certificates and certificate revocation lists. Contrast: Registration Authority.

Elector: A component of the SCMS that manages trust of Root Certificate Authority (Root CA) certificates and peer Elector certificates.

End Entity (EE): An actor that uses digital certificates to authorize application activities. Contrast: Certificate Authority (CA).

End Entity Node: A bottom-layer node in a binary hash tree used to calculate an Activation Codes for Pseudonym Certificates (ACPC) private activation value (APrV).

Enrollment Certificate: A certificate that is used to request authorization certificates and to manage other interactions between an EE and the SCMS. Contrast: authorization certificate.

Enrollment Certificate Authority (ECA): A Certificate Authority (CA) that issues enrollment certificates.

Expansion Function: A function used to produce cocoon keys from a caterpillar key in the butterfly key process.

Identification Certificate: An authorization certificate that is constructed so as not to deliberately obscure the real-world identity of the certificate holder. Contrast: pseudonym certificate.

Identifying Uniform Resource Locator (URL): A resource locator that acts as a long-lived identifier for an SCMS component.

IEEE Registration Authority (IEEE RA): A unit of IEEE that assigns unambiguous names to objects in a way that makes the assignment available to interested parties.

Indirect Authorization (for enrollment certificate request): A mode of authorization for enrollment certificate request where the enrollment certificate request generated by an EE device does not contain a proof that the device is entitled to that enrollment certificate, and the proof is instead provided to the ECA by some other means.

Individual Certificate Request: A request for a CA to issue a single certificate. The request may come from the relevant EE or from the RA. Contrast: butterfly key certificate request.

Intermediate Certificate Authority (ICA): A CA whose certificate was issued by another CA and whose main responsibility is to issue certificates to another CA, that is, an ACA, ECA, or another ICA.

i-period: A validity period for a certificate, identified by an i-value to simplify management of temporal sequences of certificates issued to an EE.

i-period epoch: The date at which i-periods of the indicated length started.

i-period length: The length of time that an i-period lasts.

i-period series: A series of temporal intervals, each of the same length, identified by an i-value that increases by one for each successive interval.

ITU-T X.509 certificate: A digital certificate following the format specified in ITU-T Recommendation X.509.

i-value: An integer identifying an i-period.

j-value: An integer identifying the index within an i-period.

Linkage Authority (LA): A component of the SCMS that provides inputs to the linkage value calculation process to enable efficient revocation of pseudonym certificates while preserving the privacy of an EE against the ACA.

Location Obscurer Proxy (LOP): A component of the SCMS that is responsible for hiding location information of an EE from the RA.

Minimal Length Hex Encoding (of an integer): The encoding of an integer with the minimum necessary number of hexadecimal characters. For example, an i-value of 76 is encoded as 0x4C. Examples of quantities that will be subject to minimal length hex encoding include i-values, j-values, and Provider Service Identifiers (PSIDs).

Misbehavior Authority (MA): A component of the SCMS that receives reports of malicious or potentially malicious application activities, analyzes them, and determines whether or not to take mitigating actions.

Omitted Node: A node in a binary hash tree whose value is omitted from the encoding of the binary hash tree and whose value cannot be derived from published nodes. Contrast: published node.

Parent Enrollment Certificate: An enrollment certificate that maintains continuity of ownership with a subsequent enrollment certificate (a successor enrollment certificate), such that if a certificate management activity could be authorized with the parent enrollment certificate that same activity can also be authorized with the successor enrollment certificate.

Physically Secure Session: A communications session in which security is provided by the fact that both endpoints of the session are in the same physically secure environment.

Privacy Against Insiders: A property of a system such that the system protects users of the system from having personal information revealed even to privileged actors within that system.

Private Key: A cryptographic key, used for key exchange, decryption, and/or signature generation, that has a corresponding public key such that the private key cannot feasibly be derived from the public key using public information.

Pseudonym Certificate: An authorization certificate that is designed to help protect the privacy of an EE. This is achieved using mechanisms such as linkage valued-based revocation. An EE that uses pseudonym certificates will typically have multiple certificates valid at the same time to allow that EE to use different certificates at different times and locations, disrupting an eavesdropper's ability to track them.

Public Key: A cryptographic key, used for key exchange, encryption, and/or signature verification, that has a corresponding private key such that the private key cannot feasibly be derived from the public key using public information.

Public Key Infrastructure (PKI): A system of certificate authorities and supporting entities to support the management of digital certificates and public keys.

Published Node: A node in a binary hash tree whose value is published in the encoding of the binary hash tree or can be derived from the values of other published nodes. Contrast: omitted node.

Registration Authority (RA): A component of the SCMS that is the main point of contact for an EE, and is responsible for provisioning the EE with authorization and successor enrollment certificates. Contrast: Distribution Center (DC), IEEE Registration Authority (IEEE RA).

Relying party: A participant of the ecosystem, who is consuming the signed datasets provided by the ecosystem.

Root Certificate Authority (Root CA): A CA that issues certificates for other entities and whose certificate was issued by itself.

Security Credential Management System (SCMS): A system of certificate authorities and supporting entities to support distribution of trust in a system based on IEEE 1609.2 digital certificates.

Security Credential Management System Manager Organization (SCMSMO): A role aimed at governing the entire SCMS, including defining and enforcing the certificate and security policies to be applied to Electors and Root CAs.

Successor Enrollment Certificate: An enrollment certificate that maintains continuity of ownership with a previous enrollment certificate (a parent enrollment certificate), such that if a certificate management activity could be authorized with the parent enrollment certificate that same activity can also be authorized with the successor enrollment certificate.

Transport Layer Security (TLS): A security protocol developed and maintained by the Internet Engineering Task Force (IETF) providing confidentiality, integrity, and authentication services.

Validity Period (of a certificate): The time period during which a certificate is to be trusted. In the IEEE 1609.2 system, this is indicated by the validityPeriod field in the certificate, that is, the time period starting at validityPeriod.start and ending at (validityPeriod.start + validityPeriod.duration).

Acronym or abbreviation	Meaning
ACPC	Activation Codes for Pseudonym Certificates
ACA	Authorization Certificate Authority
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
API	Application Programming Interface
APrV	Activation Codes for Pseudonym Certificates (ACPC) private activation value
APuV	Activation Codes for Pseudonym Certificates (ACPC) public activation value
ASD	Aftermarket Safety Device
AT	Access Token
CA	Certificate Authority
CAM	Certificate Access Manager
CAMP	Crash Avoidance Metrics Partners LLC
CAL	Certificate Access List
CCF	Certificate Chain File
CCG	Client Credentials Grant
C-OER	Canonical Octet Encoding Rules
CRACA	Certificate Revocation Authorizing Certificate Authority
CRL	Certificate Revocation List
CTL	Certificate Trust List
DC	Distribution Center
DCM	Device Configuration Manager
DER	Distinguished Encoding Rules
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ECA	Enrollment Certificate Authority
ECC	Elliptic Curve Cryptography
EE	End Entity
ECDSA	Elliptic Curve Digital Signature Algorithm

HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
I2V	Infrastructure-to-Vehicle
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITS	Intelligent Transportation Systems
JSON	JavaScript Object Notation
JWKS	JavaScript Object Notation (JSON) Web Key Set
JWT	JavaScript Object Notation (JSON) Web Token
LA	Linkage Authority
LOP	Location Obscurer Proxy
LV	Linkage Value
M2M	Machine-to-Machine
NAT	Network Address Translation
OAS	OAuth Authorization Server
OBU	On-board Unit
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OER	Octet Encoding Rules
OID	Object Identifier
P2PCD	Peer-to-Peer Certificate Distribution
PCA	Pseudonym Certificate Authority
PKI	Public Key Infrastructure
PLV	Pre-linkage Value
PSID	Provider Service Identifier
RA	Registration Authority
REST	Representational State Transfer
RFC	Request for Comments
RSU	Roadside Unit
SAS	Supplementary Authorization Server

SCMS	Security Credential Management System
SCMSMO	Security Credential Management System Manager Organization
SPDU	Secured Protocol Data Unit
SSME	Security Services Management Entity
SSP	Service Specific Permissions
TLS	Transport Layer Security
URL	Uniform Resource Locator
USDOT	United States Department of Transportation
UTC	Coordinated Universal Time
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
WAVE	Wireless Access in Vehicular Environments
WSA	Wireless Access in Vehicular Environments (WAVE) Service Advertisements

2. Publication and repository responsibilities

2.1. Methods for the publication of certificate information

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

https://autocrypt.io/services/v2x-pki-ca

- V2X PKI Certification Practice Statement
- Root CA certificate and issued subordinate authority certificate
- CRL storage location for obtaining Certificate Discard List (CRL) information
- Certification Task Information

2.2. Time or frequency of publication

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. AutoCrypt published their CRLs 24 hours after a status change via DC and/or RA.

2.3. Access controls on repositories

AutoCrypt implements access controls for the modification and management of all repositories operated by the SCMS Provider, including Distribution Center repositories.

Access control mechanisms for these repositories are implemented in compliance with the general standards for secure information handling as defined in WebTrust for Certification Authorities (WTCA v2.2.2) and ISO/IEC 27001.

AutoCrypt restricts access to repository systems to authorized personnel only, and enforces strict controls over the creation, modification, and deletion of access privileges. All access activities are logged and monitored to ensure accountability and traceability.

AutoCrypt supports strong authentication mechanisms for repository access, which are defined and documented in this CPS, in accordance with applicable security policies and regulatory requirements.

3. Identification and authentication

3.1. Naming

3.1.1. Types of names

The id field of the V2X certificate issued by the Root CA includes the following contents according to the IEEE 1609.2.1 certificate profile standard.

3.1.1.1 Names for Root CAs

The submitted CA name must be verified by the SCMS Manager to ensure that it does not conflict with any other existing names.

rootca.v2x.autocrypt.io

3.1.1.2 Identification of certificates

A certificate following the IEEE 1609.2 format shall be identified by its HashedId8 value.

3.1.2. Need for names to be meaningful

No stipulation.

3.1.3. Anonymity and pseudonymity of end-entities

An authorization certificate shall not contain any name or information that links the subject to its real identity. The ACA and RA responsible for this.

3.1.4. Rules for interpreting various name forms

No stipulation.

3.1.5. Uniqueness of Names

1. The Root CA, ICA, ACA, LA, MA names shall be unique.

2. The canonical IDs for End Entities shall be unique.

3. The SCMS Manager Organization shall ensure that a Root CA 3-byte hash certificate identifier (HashedId3) is unique in the scope of the overall trust model.

4. The SCMS Provider of Root CA and ICA shall ensure that the HashedId8 certificate identifier of each SubCA is unique.

5. The enrollment certificate’s HashedId8 shall be unique within the issuing ECA.

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. Initial identity validation

3.2.1. Method to prove possession of 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.

Key owner	**The actor responsible for the verification**	**Comments**
Root CA	SCMS Manager	self-signed IEEE 1609.2 certificate
ICA	Root CA	
ECA	ICA	
RA	ICA	
ACA	ICA	
RA	ICA	
LA	ICA	
MA	ICA	
CRL Signer	Corresponding CA	
DC	Corresponding CA	

3.2.2. Authentication of organization identity

3.2.2.1 Authentication of SubCAs organization identity

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. Authentication of individual entity

3.2.3.1 Authentication of SubCA/Other SCMS Model Elements Individual Entity

For the authentication of an individual entity (physical person) identified in association with a legal person or organizational entity (e.g., the subscriber), evidence shall be provided of:

1. full name of the subject (including surname and given names, in line with the applicable law and national identification practices);

2. date and place of birth, reference to a nationally recognized identity document or other attributes of the subscriber that may be used, as far as possible, to distinguish the person from others with the same name;

3. full name and legal status of the associated legal person or other organizational entity (e.g. the subscriber);

4. any relevant registration information (e.g. company registration) of the associated legal person or other organizational entity;

5. evidence that the subject is associated with the legal person or other organizational entity. Submitted evidence may be in the form of paper or electronic documentation.

To verify their identity, the authorized representative of a SCMS model elements or subscriber shall provide documentation proving that he/she works for the organization (certificate of authorization). He/she shall also show an official ID.

For the initial enrollment certificate process, a representative of the SubCA or other SCMS model elements shall provide the corresponding issuing CA with all necessary information. The personnel at the Root CA / ICA shall verify the identity of the certificate applicant representative and all associated documents, applying the requirements of 'trusted personnel' (The process of validating application information and generating the certificate by the Root CA / ICA shall be carried out by 'trusted persons' at the Root CA / ICA, under at least dual supervision, as they are sensitive).

3.2.4. Non-verified subscriber information

No stipulation.

3.2.5. Validation of Authority

Certificates issued by the Roots are only be issued with the PA's approval of a certificate request work order. The CA validates the authority of all certificate issuance or revocation requests from external entities as coming from an authorized representative of the organization using the information provided in sections 3.2.2 and 3.2.3.

3.2.6. Criteria for interoperation

AutoCrypt V2X Root CA implementation is compliant with the IEEE 1609.2.1 standard.

In addition, AutoCrypt continuously monitors updates to relevant standards and policies related to SCMS and V2X security, and reflects applicable changes in its certification practices to maintain interoperability with other trusted participants.

3.3. Identification and authentication for rekey requests

3.3.1. Identification and authentication for standard re-key requests

3.3.1.1 ICA, ECA, RA, ACA, LA, MA, CRL signer, DC certificate renewal or re-keying

The identification and authentication method covering routine re-keying for other SCMS model elements/entities shall be the same as that for the issuance of an initial CA certificate validation.

3.3.1.2 End Entities' enrolment credentials

Prior to the expiry of an existing enrollment certificate, the EE shall request a successor certificate to maintain continuity of certificate usage. The EE shall generate a new key pair to replace the expiring one and request a successor certificate containing the new public key; the request shall be signed with the current valid enrollment certificate private key.

The EE shall sign the enrollment certificate request with the newly created private key (inner signature) to prove delivery/possession. The EE shall then sign the whole request ('oversigned') with the current valid private key (outer signature) and encrypted to the receiving RA or ECA as specified in IEEE 1609.2.1, to ensure the confidentiality, integrity and authenticity of the request.

3.3.1.3 End Entities' authorization certificates

The certificate re-key for authorization certificates is based on the same process as the initial authorization.

3.3.2. Identification and authentication for re-key requests 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.

3.3.2.1 CA certificates

The identification and authentication process for a Root CA and a Sub-CA certificate re-keying after revocation is handled in the same way as the initial issuance of that certificate.

3.3.2.2 End Entity certificates

The authentication of an End Entity for enrollment or authorization certificate re-keying after revocation shall be handled in the same way as the initial issuance of that certificate.

3.4. Identification and authentication for revocation request

3.4.1. Root CA certificates

Revocation requests may be triggered by internal CA processes or by an external entity with legal standing and authority to make such a request. The procedures to authenticating a revocation request including followings,

Acceptable procedures for authenticating a subscriber's revocation requests include:

- a written and signed message on corporate letter paper from the subscriber requesting revocation, with reference to the certificate to be revoked,

- communication with the SCMS Provider providing reasonable assurances that the person or organization requesting revocation is in fact the subscriber; depending on the circumstances, such communication may include one or more of the following: e-mail, postal mail or courier service.

3.4.2. ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC certificates

Requests to revoke ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC certificates shall be authenticated by the issuing CA.

Acceptable procedures for authenticating a subscriber's revocation requests include:

- a written and signed message on corporate letter paper from the subscriber requesting revocation, with reference to the certificate to be revoked,

- communication with the SCMS Provider reasonable assurances that the person or organization requesting revocation is in fact the subscriber; depending on the circumstances, such communication may include one or more of the following: e-mail, postal mail or courier service.

3.4.3. End Entity enrollment certificates and authorization certificates

A request to revoke an EE enrollment certificate can originate from the EE subscriber or from MA. If initiated by the subscriber, requesters shall authenticate themselves with the MA.

A request to revoke an EE authorization certificate can originate from the EE subscriber or from MA. If initiated by the subscriber, the requester shall authenticate themselves with the MA.

4. Certificate lifecycle operational requirements

4.1. Certificate application

The certificate application shall be validated and also the identity of person submitting the application shall be verified.

4.1.1. Who can submit a certificate application

4.1.1.1 Root CA

Root CAs shall generate their own key pairs and issue their root certificate by themselves. A Root CA can submit a certificate application for endorsement through its designated representative to the SCMS Manager Organization.

4.1.1.2 ICA

An authorized representative of the ICA can submit the certificate request application to the relevant Root CA.

4.1.1.3 ECA, RA, ACA, LA, MA, DC

An authorized representative of ECA, RA, ACA, LA, MA, DC can submit the certificate request application to the relevant ICA

4.1.1.4 CRL Signer

An authorized representative of a CRL Signer can submit the certificate request application to the authorized representative of the relevant CRACA.

4.1.2. Enrollment Process and Responsibilities

Permissions for root-CAs and SubCAs issuing certificates for special (governmental) purposes (i.e. special mobile and fixed EEs) where restricted by law may be granted only by the relevant authority having jurisdiction granted by legislation to authorize the requested credentials.

4.1.2.1 Root CAs

After being audited, Root CAs may apply for insertion of their certificate(s) in the CTL.

The enrolment process is based on a signed application that shall be securely delivered to the SCMS Manager by the Root CA's authorized representative.

The Root CA's application form shall be signed by its authorized representative.

In addition to the application form, the Root CA's authorized representative shall provide its audit results to the SCMS Manager for approval. If approved, the SCMS Manager generates and sends a certificate of conformity to the corresponding Root CA.

The addition of the Root CA to the CTL is an SCMS Manager-defined internal process handled by the CTL Committee.

4.1.2.2 ICA

After being audited, the ICA may request a certificate from the Root CA.

If the ICA is owned by a different entity than the Root CA, before issuing an ICA certificate request, the ICA's entity shall have a contract with the Root CA service.

- Submission of Certificate Request: The ICA shall generate a Certificate Signing Request (CSR) in accordance with the defined profile and cryptographic standards. The generated request must be securely transmitted to the Root CA.
- Verification and Approval: The Root CA performs a comprehensive validation of the ICA's identity, authorization, and technical compliance before approving the issuance of the ICA certificate.
- Certificate Issuance: Upon successful verification, the Root CA issues the ICA certificate, which is then installed in the ICA's secure environment for further operations.

4.1.2.3 ECA, RA, ACA, LA, MA, CRL Signer, DC

After being audited, the ECA, RA, ACA, LA, MA, CRL Signer, DC may request a certificate from the ICA.

If the ECA, RA, ACA, LA, MA, CRL Signer, DC is owned by a different entity than the ICA, before issuing a certificate request, the Sub-CA or other SCMS element entity shall have a contract with the ICA service provider

4.1.2.4 End Entity

The EE subscriber shall store the proof of certification for each device type that is enrolled at an ECA or X.509 CA.

The EE may generate an enrollment certificate key pair and create an enrollment certificate request in accordance with IEEE 1609.2.1.

During the enrollment of a normal EE (as opposed to a special mobile or fixed EE), the Enrollment CA shall verify that the permissions in the initial request are not for governmental use. Such permissions are defined by the corresponding governmental entity. The detailed procedure for EE subscriber registration at the Enrollment CA shall be set out in the corresponding CPS of the ECA.

Regular EEs should be enrolled at a single Enrollment CA and therefore bound to a single RA for all certificates with a particular set of permissions. Special-purpose vehicles (such as police cars and other vehicles with specific rights) may be processed by an additional Enrollment CA or enroll for authorization within the scope of the 'special purpose'. Vehicles to which such an exemption applies shall be defined by the responsible governmental entity. Permissions for special mobile and fixed EEs shall be granted only with the approval of a jurisdictionally relevant government entity. The CPS of Root CAs or Sub-CAs issuing certificates for such special-purpose EEs shall determine the applicable enrollment process.

If the EE is in the process of migrating from one Enrollment CA to another, it is permitted to be enrolled at two

CAs simultaneously for that period.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

4.2.1.1 Identification and authentication of Root CAs

The SCMS Manager is responsible for authenticating the Root CA's authorized representative and approving its application. The application approval shall be done by the CTL committee.

The SCMS Manager shall confirm its positive validation of the application to the Root CA/Elector. The Root CA may then send its 'self-signed' certificate to the SCMS Manager, which shall add the certificate of Root CA to the CTL.

4.2.1.2 Identification and authentication of the ICA

AutoCrypt V2X Root CA is responsible for authenticating the ICA's authorized representative and approving its application.

AutoCrypt V2X Root CA confirm its positive validation of the application to the ICA. The ICA may then send a certificate request to the Root CA, which shall issue the certificate to the corresponding ICA.

4.2.1.3 Identification and authentication of ECA, RA, ACA, LA, MA, DC

The corresponding ICA is responsible for authenticating the Sub-CA's or other SCMS element authorized representative and approving its application.

The ICA shall confirm its positive validation of the application to the respective Sub-CA or other SCMS element. The Sub-CA or other SCMS element may then send a certificate request to the ICA, which shall issue the certificate to the corresponding Sub-CA or other SCMS element.

4.2.1.4 Identification and authentication of CRL signer

The corresponding CRACA is responsible for authenticating the CRL Signer's authorized representative and approving its application.

The corresponding CRACA shall confirm its positive validation of the application to the respective CRL Signer. The CRL Signer may then send a request to the CRACA which shall issue the certificate to the corresponding CRL Signer.

4.2.1.5 Identification and authentication of EE subscriber

The ECA is responsible for authenticating the EE subscriber. The Enrollment CA (SCMS ECA or X.509 CA) shall describe in its CPS the processes for EE subscriber authentication.

The ECA shall confirm its positive validation of the application to the respective EE subscriber. The EE may then send a certificate request to the ECA, which shall issue the certificate to the corresponding EE.

4.2.1.6 Identification and authentication of EE

During enrollment-stage certificate requests, the ECA shall use at least one of the authentication options in accordance with IEEE 1609.2.1.

During successor enrollment certificate requests and downloads, the RA shall use at least one of the authentication options for both EE and RA in accordance with IEEE 1609.2.1.

During authorization certificate requests and downloads, in accordance with IEEE 1609.2.1, the RA shall verify the EE's enrollment certificate and authenticate the ECA or X.509 CA from which the EE received its enrollment certificate. If the RA is not able to authenticate the EE and ECA or X.509 CA, the request shall be rejected. The RA shall use at least one of the authentication options for both EE and RA in accordance with IEEE 1609.2.1.

During misbehavior report submission, the RA shall use at least one of the authentication options in accordance with IEEE 1609.2.1.

4.2.2. Approval or rejection of certificate applications

4.2.2.1 Approval or rejection of Root CA certificates

The SCMS Manager CTL Committee adds/removes the Root CA certificate to/from the CTL, when it is clear from the audit results and the CPS that the Root CA/Elector is in compliance with this CP.

4.2.2.2 Approval or rejection of ICA certificates

The Root CA shall verify the ICA certificate request based on its audit results. If this verification leads to a positive result, the Root CA may issue a certificate to the requesting ICA.

4.2.2.3 Approval or rejection of ECA, RA, ACA, LA, MA, DC certificates

The ICA shall verify the Sub-CAs or other SCMS element certificate request based on its audit results. If this verification leads to a positive result, the ICA may issue a certificate to the requesting entity.

4.2.2.4 Approval or rejection of CRL Signer certificates

The CRACA shall verify the CRL Signer certificate request based on its audit results. If this verification leads to a positive result, the CRACA may issue a certificate to the requesting entity.

4.2.2.5 Approval or rejection of enrollment certificate

The Enrollment CA shall verify and validate enrollment certificate requests. If this verification leads to a positive result, the ECA may issue a certificate to the requesting entity.

4.2.2.6 Approval or rejection of authorization certificate

The RA shall verify and validate authorization certificate requests. If this verification leads to a positive result, the ACA may issue a certificate to the requesting entity.

The RA and the ACA shall accept and approve authorization requests if the following are fulfilled:

(a) actual, valid and relevant CRL and CTL are available at RA/DC,

(b) the Root CA certificate and ICA certificate of the CA's certificate chain were not revoked,

(c) Root CA certificate is listed on the actual, valid and relevant CTL.

4.2.3. Time to process the certificate application

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.

4.2.3.1 Root CA certificate application

The time to process the identification and authentication process of a Root CA certificate application is 60 working days.

4.2.3.2 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC certificate application

The time to process the identification and authentication process of a certificate application is during working days in accordance with the agreement and contract between the Root CA and the ICA, and between the ICA and the SubCA or other SCMS element

4.2.3.3 Enrollment certificate application

The processing of enrollment certificate applications should be subject to a maximum time limit laid down in the ECA's CPS. This shall not be - at normal conditions - more than 5 days.

4.2.3.4 Authorization certificate application

The processing of authorization certificate applications shall be subject to a maximum time limit laid down in the RA's and ACA's CPS. This shall not be - at normal conditions - more than 15 minutes.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

4.3.1.1 Root CA certificate issuance

The Root CA shall issue its own self-signed Root CA certificate in IEEE 1609.2.1 format and may send it to the SCMS Manager for publication on the CTL.

4.3.1.2 ICA certificate issuance

The Root CAs shall issue ICA certificates in IEEE 1609.2.1 format.

The Root CA shall check the audit results of the ICA before issuing a certificate for it.

The Root CA shall take care that the ICA certificate is made available via RA repository or DC as soon as needed

4.3.1.3 CRL Signer certificate issuance

The CRACA may issue CRL Signer certificates in IEEE 1609.2.1 format.

The CRACA shall check the audit results of the CRL Signer before issuing a certificate for it.

The CRACA shall take care that relevant CRL Signer certificates are made available via RA and DC if the CRL Signer certificate is not included in the CRL itself.

4.3.1.4 ECA, RA, ACA, LA, MA, DC certificate issuance

The ICA shall issue ECA, RA, ACA, LA, MA, DC certificates in IEEE 1609.2.1 format.

The ICA shall check the audit results of the ECA, RA, ACA, LA, MA, before issues certificate for it.

The ICA shall take care that relevant ECA, RA, ACA, LA, MA, DC certificates are made available via RA repository or DC.

4.3.1.5 Enrollment certificate issuance

The Enrollment CA shall issue enrollment certificates in IEEE 1609.2.1 or X.509 format following RFC 5280 and RFC 5480.

The Enrollment CA shall evaluate the enrollment certificate request to ensure that all fields are correct and valid. After successful validation, the Enrollment CA shall issue the certificate or otherwise reject the certificate request.

Enrollment certificate requests and responses shall be encrypted to ensure confidentiality, and signed to ensure authentication and integrity.

4.3.1.6 Authorization certificate issuance

The ACA shall issue authorization certificates in IEEE 1609.2.1 format.

The ACA shall make available the authorization certificates to the EE via RA interface.

Authorization certificate requests and responses shall be encrypted to ensure confidentiality, and signed to ensure authentication and integrity.

4.3.2. CA's notification to subscriber of issuance of certificates.

Not applicable.

4.4. Certificate acceptance

4.4.1. Conducting certificate acceptance

4.4.1.1 Root CA

Not applicable.

4.4.1.2 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC

The SubCA or other SCMS model element verifies the certificate type (ScmsSsp), the signature and the information in the received certificate. The SubCA or other SCMS model element discard all enrollment/authorization certificates that are not correctly verified and issue a new request.

Acceptance may be deemed to occur if the CA does not receive any notice from the subscriber within a certain time period.

After the Root CA issues a certificate to an ICA or other SubCA, the following steps are performed to ensure secure delivery and proper acceptance in compliance with V2X-specific requirements:

The Root CA generates the certificate using the IEEE 1609.2 standard, encoded in OER (Octet Encoding Rules) format. The certificate includes the necessary fields defined for V2X use, such as issuer, subject, validity period, and permissions.

The generated certificate is delivered to the ICA or subordinate CA via a secure and authenticated channel.

Acceptable transmission methods include: SFTP, Authenticated HTTPS API, Physical delivery of an encrypted medium (e.g. USB driver)

To ensure the integrity of the certificate, a cryptographic hash (e.g., SHA-256) of the certificate may be sent to the recipient CA through a trusted out-of-band channel (e.g., separate email, or postal mail).

Upon receipt, the ICA shall Confirm that all certificate fields are correct and aligned with the agreed profile.

4.4.1.3 End Entity

The EE shall verify the received enrollment and authorization certificates against its original request, including the signature and certificate chain.

It shall discard all EC/AC responses that are not correctly verified. In such cases, it should send a new enrollment/authorization certificate request.

4.4.2. Publication of the certificate

Root CA certificates shall be made available to all participants through CTLs via the SCMS Manager's PUB.

Sub-CAs' or other SCMS model element certificates shall be published by the issuing CA.

Enrollment and authorization certificates shall not be published.

ICA, ACA, and CRL Signer certificates may be published by the EE via P2PCD according to IEEE 1609.2.1.

4.4.3. Notification of certificate issuance

Where applicable, the CA notifies relevant stakeholders of certificate issuance via email and by updating certificate chain files used in automated management processes defined in IEEE 1609.2 and SCMS architecture specifications.

4.5. Key pair and certificate usage

4.5.1. Private key and certificate usage

4.5.1.1 Private key and certificate usage for Root CA

The Root CA shall use its Root CA private keys to sign its own (Root CA) certificates, CRLs, and Sub-CAs.

The Root CA certificate shall be used by PKI participants to verify the CRL and the Sub-CAs certificate.

4.5.1.2 Private key and certificate usage for ICA

The ICA shall use its CA private keys to sign its own CSR and the certificates for ECA, RA, ACA, LA, MA, CRL Signer, DC, and CRLs.

The ICA certificates shall be used by SCMS model elements and EEs to verify certificates and CRLs where the ICA is the issuer.

4.5.1.3 Private key and certificate usage for ECA

The ECA shall use its CA private keys to sign its own CSR and enrollment certificate.

According to IEEE 1609.2.1, the ECA can use an X.509 certificate for authentication in session-based communications.

ECA certificates shall be used by SCMS model elements and end entities to verify enrollment certificates and SPDUs from the ECA.

4.5.1.4 Private key and certificate usage for RA

The RA shall use its private keys to sign its own CSR and decrypt SPDUs. Also, this certificate may be used by the RA to authenticate itself in communication with other SCMS model elements and EEs.

RA certificates shall be used by SCMS model elements and EEs to encrypt SPDUs for the RA.

4.5.1.5 Private key and certificate usage for ACA

The ACA shall use its CA private keys to sign its own CSR, authorization certificates, CRL Signer certificates, CRLs.

ACA certificates shall be used by SCMS model elements and end entities to verify authorization certificates, CRL Signer certificates, CRLs where the ACA is the issuer.

4.5.1.6 Private key and certificate usage for LA

The Linkage Authority (LA) shall use its private keys to sign its own CSR.

LA certificates may be used by SCMS model elements to authenticate the LA.

4.5.1.7 Private key and certificate usage for MA

The Misbehavior Authority (MA) shall use its private keys to sign its own CSRs and decrypt misbehavior reports.

MA certificates may also be used by SCMS model elements to authenticate the MA in communication.

4.5.1.8 Private key and certificate usage for CRACA and CRL Signer

The CRACA and CRL Signer shall use its private keys to sign its own CSRs and CRLs.

CRACA and CRL Signer certificates shall be used by SCMS model elements and EEs to verify the CRLs.

4.6. Relying party public key and certificate usage

Parties relying on the public keys use the trusted certification path for the purposes referred to in the certificates and to authenticate the trusted common identity of enrollment/authorization certificates.

Certificates in the SCMS model shall not be used without a preliminary check by a party replying on them.

4.7. Certificate renewal

Not allowed.

4.8. Certificate re-key

4.8.1. Circumstances for certificate re-key

Certificate re-key shall be processed when a certificate reaches the end of its lifetime or a private key reaches the end of operational use, but the trust relationship with the CA still exists. A new key pair and the corresponding certificate shall be generated and issued in all cases.

4.8.2. Who may request re-key

4.8.2.1 Root CA

Root CA does not request a re-key. The re-keying process is an internal process for the Elector and Root CA because its certificate is self-signed.

4.8.2.2 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC

The CA issuing the Sub-CA or other SCMS element certificate shall specify in its CPS whether re-keying is supported or not.

The re-keying request shall be submitted well before the current Sub-CA or other SCMS element certificate expires, allowing enough time for the new certificate and operational key pair to be approved and issued.

4.8.2.3 End Entity

The EE shall re-key its enrollment certificate according to IEEE 1609.2.1.

4.8.3. Re-keying process

4.8.3.1 Elector and Root CA

Not applicable.

4.8.3.2 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC

The Sub-CA or other SCMS element may request a new certificate or a re-key certificate as follows: The Sub-CA or other SCMS element shall generate a new key pair to replace the expiring key pair and sign the re-key request containing the new public key with the current valid private key ('re-keying'). The Sub-CA or other SCMS element shall generate a new key pair and sign the

request with the new private key (inner signature) to prove possession of the new private key. The whole request shall be signed ('oversigned') with the current valid private key (outer signature) to ensure the integrity and authenticity of the request.

4.8.3.3 End Entity certificates

The EE shall re-key its enrollment certificate according to IEEE 1609.2.1.

4.9. Certificate modification

Not allowed.

4.10. Certificate revocation and suspension

4.10.1. Circumstances for revocation

Certificate revocation may be performed for the following circumstances:

(a) if the SCMS Manager has reason to believe or strongly suspects that the corresponding Elector/Root CA private key has been compromised,

(b) if the issuing CA (Root CA or Sub-CA) has a reason to believe that the private key associated with that certificate has been compromised,

(c) if the audit (see Section 8) leads to a negative result,

(d) if the Sub-CA/End Entity is no longer associated with the EE subscriber or the organization managing the Sub-CA,

(e) if there is incorrect information included in the certificate which may cause it to be used or relied upon inappropriately,

(f) if the subscriber agreement has been terminated,

(g) if the subscriber has violated its license or certificate usage agreements,

(h) if ordered by a court or entity with contractual or legal jurisdiction.

Enrollment certificates and authorization certificates shall be revoked for loss or suspected compromise of the EE, application or private key.

4.10.2. Who can request revocation

SCMS Manager can trigger the removal of an Elector or Root CA from the CTL.

The Root CA is a self-signed certificate, so removal from the CTL can only be requested by these entities via the SCMS Manager.

The Sub-CA representative can request the revocation of its own Sub-CA certificates.

The issuing CA can trigger the revocation of the certificates issued by itself.

The EE subscriber representative can request the revocation of certificates requested by itself.

EE subscriber and MA can request the revocation of EE certificates which they are responsible for.

CAs shall accept revocation requests from all authorized and authenticated parties, such as an authorized representative of the United States Department of Transportation (USDOT).

CAs may establish procedures that allow other entities to request certificate revocation for fraud or misuse. A CA Provider may revoke a certificate of its own volition to safeguard the trust in the SCMS Manager ecosystem even if no other entity has requested revocation, after a threeday notice to the Subscriber and the SCMS Manager, unless a shorter time period is necessary due to critical/urgent circumstances.

Demonstrated key compression can be reported by anyone.

4.10.3. Procedure for revocation request

4.10.3.1 Removal of a Root CA

A Root CA shall be removable from CTL. In the event of removal, the SCMS Manager shall publish a new CTL as soon as possible and without undue delay.

The Root CA removal from the CTL is the responsibility of SCMS Manager's CTL Committee, as defined in its internal processes.

The Root CA shall immediately notify the SCMS Manager of a known or suspected compromise of their private key. It must be assured that only authenticated requests result in certificate removal.

4.10.3.2 Revocation of ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC certificates

An ICA, ECA, RA, ACA, LA, MA, CRL Signer, and DC certificate shall be revocable. The Root CA shall process the revocation request, under normal conditions, within 5 days. If the revocation cause is the compromise of the key, this revocation shall be done as soon as possible.

Revoked certificates shall be published on a CRL within 24 hours.

The CRACA or CRL Signer shall update, sign and publish the CRL within 24 hours to the DC.

The Sub-CA and the other SCMS element shall immediately notify the issuing CA of a known or suspected compromise of its private key. It must be assured that only authenticated requests result in revoked certificates.

4.10.3.3 Revocation of enrollment certificates

An enrollment certificate can be blocked. If the certificate is blocked by the ECA or RA or supplementary Authorization Server, it shall not be accepted for any usage.

The ECA shall process the blocking/revocation request, under normal conditions, within 5 days. If the blocking/revocation cause is the compromise of the key, this revocation shall be done as soon as possible.

If an EE is determined by an MA to be not working correctly, the ECA, RA or supplementary Authorization Server shall change its status to 'blocked' and it shall not be accepted for any usage.

4.10.3.4 Revocation of authorization certificates

Revocation of the authorization certificates can be initiated by the CRACA using linkage Id-based revocation information or hash Id-based revocation information according to IEEE 1609.2.1 in the following cases:

(a) requested by an EE subscriber,

(b) terminated EE subscriber,

(c) requested by the MA,

(d) ordered by a court decision.

The ACA shall process the revocation request, under normal conditions, within 5 days. If the revocation cause is the compromise of the key, this revocation shall be done as soon as possible.

Activation Codes for Pseudonym Certificates (ACPC) can be used to lock authorization certificates. A locked certificate cannot be used until the (re) activation code is received by the EE.

4.10.4. Processing of misbehavior reports

MA shall process misbehavior reports only if the following requirements are fulfilled:

(a) the signature of the reporting End Entity on the MBR is valid,

(b) valid and relevant Elector certificates are available,

(c) valid and relevant CRL and CTL are available,

(d) the Root CA certificate and the ICA certificate of the MA certificate chain are valid,

(e) on the basis of the MA's own root certificate list.

4.11. Certificate status services

4.11.1. Operational characteristics

Not applicable

4.11.2. Service availability

Not applicable

4.11.3. Optional features

Not applicable

4.12. End of subscription

Not applicable

4.13. Key escrow and recovery

Not applicable

5. Facility, management and operational controls

5.1. Physical controls

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. Site location and construction

5.1.1.1 Root CA

The location and construction of the facility housing the Root CA equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request, etc.) shall be consistent with facilities used to house high value and sensitive information. Root CA shall be operated in a dedicated physical area separated from other PKI components' physical areas.

Root CA shall implement policies and procedures to ensure that a high level of security is maintained in the physical environment in which the Elector and Root CA equipment is installed, so as to guarantee that:

(a) it is isolated from public networks,

(b) the physical environment contains a series of (at least two) progressively more secure physical zones and the Root CA shall be in the most secure zone,

(c) sensitive data (HSM, key pair backup, activation data, etc.) are stored in a dedicated safe set aside in a physical area protected by multiple access controls.

The security techniques employed shall be designed to resist a large number and combination of different forms of attack. The mechanisms used shall include at least:

(a) perimeter alarms, closed circuit television, reinforced walls and motion detectors,

(b) two-factor authentication (e.g. smartcard and PIN) for every person and badge to enter and leave the Root CA facilities and safe physical secured area.

The Root CA shall use authorized personnel to monitor the facility housing core equipment. The personnel of the operational environment shall never have access to the secure areas of Root CAs or sub-CAs unless authorized.

5.1.2. Physical access

5.1.2.1 Root CA

Equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request, etc.) shall always be protected from unauthorized access. The physical security mechanisms for equipment shall at least:

(a) monitor, either manually or electronically, for unauthorized intrusion at all times,

(b) ensure that no unauthorized access to the hardware and activation data is permitted,

(c) ensure that all removable media and paper containing sensitive plaintext information are stored in a secure container,

(d) ensure that any individual entering secure areas who is non-authorized on a permanent basis shall not be left without supervision by an authorized employee of the Root CA facilities,

(e) ensure that an access log is maintained and inspected periodically,

(f) provide at least two layers of progressively increasing security, e.g. at perimeter, building and operational room level,

(g) require two trusted role physical access controls for the cryptographic HSM and activation data.

A security check of the facility housing equipment shall be carried out if it is to be left unattended. At a minimum, the check shall verify that:

(a) the equipment is in a state that is appropriate for the current mode of operation,

(b) for off-line components, all equipment is shut down,

(c) any security containers (tamperproof envelope, safe, etc.) are properly secured,

(d) physical security systems (e.g. door locks, vent covers, electricity) are functioning properly;

(e) the area is secured against unauthorized access.

Removable cryptographic modules shall be deactivated prior to storage.

When not in use, such modules and the activation data used to access or enable them shall be placed in a safe. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded to the cryptographic module. They shall not be stored with the cryptographic module, so as to avoid only one person having access to the private key.

A person or group of trusted roles shall be made explicitly responsible for making such checks. Where a group of people is responsible, a log shall be maintained that identifies the person performing each check. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date/time and confirms that all necessary physical protection mechanisms are in place and activated.

5.1.3. Power and air conditioning

The Root CA system shall be equipped with reliable access to electric power to ensure operation with no or minor failures. Primary and backup installations are required in the event of external power failure and smooth shutdown of the CITS trust model equipment in the event of a lack of power. The Root CA system facilities shall be equipped with heating/ventilation/air conditioning systems to maintain the temperature and relative humidity of the equipment within operational range.

5.1.4. Water exposures

The Root CA system should be protected in a way that minimizes impact from water exposure. For this reason, water and soil pipes shall be avoided.

5.1.5. Fire prevention and protection

To prevent damage caused by exposure to fire or smoke, the secure facilities critical to the Root CA system shall be properly constructed and equipped, and appropriate procedures shall be implemented to address fire-

related threats. Media storage shall be protected against fire using appropriate fire-resistant containers.

5.1.6. Media management

The Root CA system shall protect physical media holding backups of critical system data or any other sensitive information from environmental hazards and unauthorized use of, access to or disclosure of such media.

Media used in the Root CA system are securely handled to protect them from damage, theft and unauthorized access. Media management procedures are implemented to protect against obsolescence and deterioration of media in the period for which records have to be retained.

Sensitive data shall be protected against being accessed as a result of re-used storage objects (e.g. deleted files), which may make the sensitive data accessible to unauthorized users.

An inventory of all information assets shall be maintained and requirements set out for the protection of those assets that are consistent with the risk analysis.

5.1.7. Waste disposal

The Root CA system shall implement procedures for the secure and irreversible disposal of waste (paper, media or any other waste) to prevent the unauthorized use of, access to or disclosure of waste containing confidential/private information. All media used for the storage of sensitive information, such as keys, activation data or files, shall be destroyed before being released for disposal.

5.1.8. Off-site backup

Backups of the Root CA system, sufficient to recover from system failure, shall be performed offline after the deployment of SCMS model elements and after each new key pair generation. Backup copies of essential business information (including key pairs, CRLs, CTLs, certificates, and configurations) and software shall be created on a regular basis. Adequate backup facilities shall be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Backup arrangements for individual systems shall be regularly tested to verify that they meet the requirements of the business continuity plan. At least one full backup copy shall be stored at an off-site location for disaster recovery purposes. The off-site backup location shall be protected by physical and procedural controls commensurate with those applied to the operational PKI system.

Backup data shall be subject to the same access control requirements as operational data and shall be stored securely at the off-site location. In the event of a complete loss of data, all information required to restore SCMS model elements to operational status shall be fully recoverable from the backup data.

Private key material of the Root CA system shall not be backed up using standard backup mechanisms. Instead, private key backups shall be performed exclusively using the backup function provided by the cryptographic module.

5.2. Procedural controls

This section describes requirements for roles, duties and identification of personnel.

5.2.1. Trusted roles

Trusted roles shall include those that involve the following responsibilities:

(a) Executive Officer

- Oversee overall certification operations.
- Approve the Certificate Policy (CP) and Certification Practice Statement (CPS).
- Approve information security policies, Business Continuity Plans (BCP), and Disaster Recovery Plans (DRP).

(b) Policy Managers

- Establish and revise the Certification Practice Statement (CPS).
- Establish procedures for Business Continuity Plans and Disaster Recovery Plans.
- Create periodic training curricula for certificate management staff and conduct training.

(c) Internal Auditors

- Perform periodic internal audits on certificate issuance and management.
- Perform monthly internal audits on certificate system audit logs.
- Conduct disaster recovery drills and key validation tests.
- Supervise security management of the certificate system and services.

(d) Cryptographic Device Administrator

- Comply with procedures and detailed regulations for key generation, storage, transportation, transfer, and destruction.
- Review the usage history of key generation data related to HSMs.
- Store key generation data related to HSMs (e.g., in fireproof safes).
- Provide and manage items and information required for 'm of n' access control personnel for HSM activation.

(e) Certificate Management Officers

- Perform and manage new issuance, re-issuance, and revocation of certificates within the CA system.
- Manage the issuance of Certificate Revocation Lists (CRL).

(f) CA System Developers

- Develop and manage certification-related tasks (including Root CA systems).
- Analyze domestic and international technical standards and requirements, and apply them to

systems and applications.

(g) System Administrators

- Monitor the certification center and perform system maintenance and management.
- Manage backup and recovery of the certification system.
- Manage security inspections and facility inspections of the certification system.

(h) System Operators

- Operate the certification system and network.

5.2.2. Number of persons required per task

The Root CA system shall establish, maintain and enforce rigorous control procedures to ensure the separation of duties based on trusted roles and to ensure that multiple trusted persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure separation of duties based on job responsibilities. The most sensitive tasks, such as access to and the management of CA cryptographic hardware (HSM) and its associated key material, must require the authorization of multiple trusted persons.

These internal control procedures shall be designed to ensure that at least two trusted persons are required to have physical or logical access to the device. Restrictions on access to CA cryptographic hardware must be strictly enforced by multiple trusted persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction.

5.2.3. Identification and authentication for each role

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 requiring separation of duties

Roles requiring separation of duties include roles requiring access to sensitive areas, the activation of cryptographic modules, the generation of CA keying materials and the processing of CA certificate applications as documented in AutoCrypt V2X Root CA Operations Responsibility Matrix and CA keying ceremonies documentation.

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. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

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. Background check procedures

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
- Regular screening of identities for employees who hold positions of trust

5.3.3. Training requirements

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.

Training programs shall address matters that are relevant to the particular environment of the trainee, including:

(a) security principles and mechanisms of the SCMS model elements,

(b) all duties the person is expected to perform, and internal and external reporting processes and sequences,

(c) PKI business processes and workflows,

(d) incident and compromise reporting and handling,

(e) disaster recovery and business continuity procedures,

(f) configuration and access management of the PKI system,

(g) sufficient IT knowledge.

5.3.4. Retraining frequency and requirements

The persons assigned to trusted roles are required to refresh the knowledge they have gained from training on an ongoing basis.

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 rotation frequency and sequence

In '5.2.4 Roles requiring separation of duties', changes are made to the extent that job changes do not affect the security of the system.

5.3.6. Sanctions for unauthorized actions

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. Documentation supplied to personnel

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 logging procedures

As an offline CA, event logging only occurs when a Root-CA is activated. All operator actions are logged and reviewed following each activation by an internal auditor. The administrator is a different person from those who control the signing key. The auditor reports any unusual events to the PA for analysis and resolution. All available logs may be subject to audit by the independent auditor.

5.4.1. Types of events recorded

Security audit logs are automatically collected for access to PKI facilities. In addition to electronic logs, a visitor logbook is used to record the entrance and exit of personnel.

Electronic video and signed paper copies of keying ceremonies are archived and kept of keying ceremonies and other physical interactions with the CA.

All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

Each event related to certificate life cycle is logged in such a way that it can be attributed to the person that performed it. All data related to a personal identity are protected against nonauthorized access.

Each audit record includes the following if applicable (either recorded automatically or manually for each auditable event):

(a) trusted date and time the event occurred,

(b) result of the event . success or failure where appropriate,

(c) identity of the entity and/or operator that caused the event if applicable,

(d) identity of the entity for which the event is addressed.

Detailed list of the audit logs is listed below.

(a) physical facility access . access by physical persons to the facilities shall be recorded; an event shall be created every time a record is created,

(b) trusted roles management . any change in the definition and level of access of the different roles shall be recorded, including modification of the attributes of the roles; an event shall be created every time a record is created,

(c) logical access . an event shall be generated when an entity (e.g. a program) has access to sensitive areas (i.e. networks and servers),

(d) backup management . an event shall be created every time a backup is completed, either successfully or unsuccessfully,

(e) log management . logs shall be stored. An event shall be created when the log size exceeds a specific size,

(f) data from the authentication process for subscribers and trust model elements . events shall be generated for every authentication request by subscribers and trust model elements,

(g) acceptance and rejection of certificate requests, including certificate creation and renewal . an event shall be generated periodically with a list of accepted and rejected certificate requests in the previous seven days,

(h) manufacturer registration . an event shall be created when a manufacturer is registered,

(i) end entity events . an event shall be created when an end entity is registered and every time when registration status is changed/updated,

(j) HSM management . an event shall be created when an HSM security breach is recorded,

(k) IT and network management, as they pertain to the PKI systems . an event shall be created when a PKI server is shut down or restarted,

(l) security management . covers successful and unsuccessful PKI system access attempts, PKI and security system actions performed, security profile changes, system crashes, hardware failures and other anomalies, firewall and router activities; and entries to and exits from the PKI facilities.

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

5.4.2. Frequency of processing log

Audit logs shall be reviewed in response to alerts based on irregularities and incidents within the AutoCrypt V2X systems.

Audit log processing shall consist of a review of the audit logs and documenting the reason for all significant events in an audit log summary. Audit log reviews shall include a verification that the log has not been tampered with, an inspection of all log entries and an investigation of any alerts or irregularities in the logs. Action taken on the basis of audit log reviews shall be documented.

The audit log shall be archived at least weekly. An administrator shall archive it manually if the free disk space for audit log is below the expected amount of audit log data produced that week.

5.4.3. Retention period for audit log

Log records relating to certificate lifecycles are kept for at least five years after the corresponding certificate expires.

5.4.4. Protection of audit log

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.

Electronic audit log entries shall be signed with a secure method.

Events are logged in such a way that they cannot be easily deleted or destroyed (except for transfer to longterm media) within the period for which the logs have to be held.

Event logs are protected in such a way as to remain readable for the duration of their storage period.

5.4.5. Audit log backup procedures

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 events recorded ', 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.
- The HSM administrator keeps backed up audit logs in the fireproof safe located in Security Area #4.
- The system operator synchronizes the audit log copy to the DR center.

5.4.6. Audit collection system (internal or external)

The equipment of the SCMS model elements shall activate the audit processes at system startup and deactivate them only at system shutdown. If audit processes are not available, the SCMS model element shall suspend its operation.

At the end of each operating period and at the rekeying of certificates, the collective status of equipment should be reported to the operations manager and operation governing body of the respective PKI element.

5.4.7. Notification to event-causing subject

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 assessment

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 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 archiving

5.5.1. Types of record archiving

The Root CA archives records in sufficient detail to establish the validity of signatures and the proper operation of the PKI. All detailed records of Root CA certification work including '5.4.1 Types of events recorded' should be kept.

(a) physical facility access log of CA,

(b) trusted roles management log for CA,

(c) IT access log for CA,

(d) Key creation, use and destruction log,

(e) Certificate creation, use and destruction log,

(f) Activation data management log for CA,

(g) PKI documentation for CA,

(h) Security incident and audit report for CA,

(i) System configuration.

The Root CA retains the following documentation relating to certificate requests and their verification, as well as all SCMS model element certificates, CTLs, and related revocation information:

(a) PKI audit documentation kept by CA,

(b) CPS documents kept by CA,

(c) contract between SCMSMO and other entities kept by CA,

(d) certificates (or other revocation information) kept by the CA,

(e) certificate request records in Root CA/Sub-CA system,

(f) other data or applications sufficient to verify archive contents,

(g) all work related to or from the SCMS model elements and compliance auditors.

The Root CA retains all documentation relating to certificate requests and their verification, and all certificates and related revocation information, for at least seven (7) years after any certificate based on that documentation ceases to be valid.

5.5.2. Retention period for archive

Without prejudice to any regulations requiring a longer archival period, the AutoCrypt V2X Root CA SHALL retain all records for at least five (5) years after the corresponding certificate has expired.

5.5.3. Protection of archive

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. System archive and storage

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. Requirements for time-stamping of records

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. Archive collection system (internal or external)

No stipulation.

5.5.7. Procedures to obtain and verify archive information

All SCMS model elements shall allow only authorized/trusted persons to access the archive.

SCMS model elements shall verify the integrity of the information before it is restored.

5.6. Key changeover for trust model elements

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.

5.7. Compromise and disaster recovery

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. Incident and compromise handling

The Root CA monitors its equipment on an ongoing basis to detect potential hacking attempts or other forms of compromise. If a compromise is detected, the Root CA SHALL conduct an investigation to determine the nature and extent of the damage.

In addition, the CA entity determines which services are to be maintained and how, in accordance with the CA’s Disaster Recovery and Business Continuity Plan.

If a security incident is suspected AutoCrypt CA Operation Manager is called in to determine root cause and possible damage.

AutoCrypt Tech security incident response procedures are followed to mitigate issues. In the case of a

compromised PKI component and particularly the compromise of a private key, the CA alerts its stakeholders to allow them to also mitigate risks.

The Disaster Recovery and Business Continuity Plan is executed if required.

Supporting procedures are reviewed periodically (at least on an annual basis) and are revised and updated as needed.

5.7.2. Corruption of computing resources, software and/or data

CA personnel perform system back-ups on a regular basis. Back-up copies are made of CA Private Keys and are stored off-site in a secure location.

In the event of corruption or a disaster whereby the primary and disaster recovery CA operations become inoperative at the primary facility and the Disaster Recovery, the CA will reinitiate its operations on replacement hardware using backup copies of its software, data and CA private keys at a comparable, secured facility.

All other events shall be included in the periodic SCMS model element audit results.

5.7.3. Entity private key compromise procedures

If the private key (or its backup) of a Root CA is compromised, lost, destroyed or suspected of being compromised, the Root CA shall:

(a) suspend its operation,

(b) start the disaster recovery and migration plan,

(c) investigate the 'key issue' that generated the compromise and notify the SCMSMO, which will remove it from the CTL,

5.7.4. Business continuity capabilities after a disaster

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. Termination and transfer

This section describes the operational procedures required in the event of the termination of the Root CA

service or the migration of services to another entity, ensuring compliance with the migration plan and security requirements.

(a) Migration Planning and Approval : The Policy Manager establishes a comprehensive 'Service Migration Plan' at least six (6) months prior to the projected termination date. This plan includes the scheduled termination date, impact analysis for subscribers and subordinate CAs (ICAs), measures to maintain certificate validity, and procedures for transferring the CRL and audit logs. The plan guarantees ongoing operation for all subscribers and takes effect only after obtaining final approval from the Executive Officer.

(b) Notification and Coordination : At least 90 days prior to the termination date, the Executive Officer notifies the Superior CA (if applicable) and the SCMSMO of the termination plan via an official written notice. Concurrently, the Certificate Management Officer officially requests the SCMS Manager to remove the Root CA certificate from the Certificate Trust List (CTL) effective upon the service termination date. The Policy Manager also alerts other Root CAs and SCMS Providers with whom agreements exist regarding the re-keying of ICA certificates and CRL Signer certificates.

(c) Final CRL Issuance : Immediately prior to the termination of service, the Certificate Management Officer generates and digitally signs the final Certificate Revocation List (CRL). The System Administrator publishes this CRL to the repository, clearly indicating that it contains the 'latest revocation information' and that no further CRLs will be issued.

(d) Key Destruction : The Cryptographic Device Administrator performs a 'Key Destruction Ceremony' to permanently destroy the Root CA private keys stored in the Hardware Security Module (HSM), as well as all backup copies (e.g., smart cards, USB drives) and activation data. This process is strictly witnessed and verified by the Internal Auditor to ensure the keys are rendered unrecoverable.

(e) Records Archiving and Transfer : The System Administrator backs up and archives all audit logs, certificate issuance records, and policy documents generated prior to the service termination. Subsequently, the Executive Officer ensures that these archived records are securely transferred to the SCMS Manager in accordance with the specified procedures, obtaining a confirmation of receipt upon completion.

6. Technical security controls

6.1. Key pair generation and installation

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 140-3 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.
- The CA does not generate Subscriber key pairs.

6.1.1. Cryptographic requirements

The following table shows the mandatory algorithm implementations for certificate type and for usages: (Specified by NIST FIPS 186-4 and RFC 5639, defined in IEEE 1609.2 and IEEE 1609.2.1)

	ecdsaBrainpool P256r1 WithSha256	**ecdsaBrainpool P384r1 WithSha384**	**ecdsaNist P256 WithSha256**	**ecdsaNist P384 WithSha384**
Root CA	signing/verification	signing/verification	signing/verification	signing/verification
ICA	signing/verification	signing/verification	signing/verification	signing/verification
ECA	signing/verification	signing/verification	signing/verification	signing/verification
ACA	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption
CRL Signer	signing/verification	signing/verification	signing/verification	signing/verification
RA	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption
LA	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption
MA	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption
DC	signing/verification	signing/verification	signing/verification	signing/verification

EC	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption
AC	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption

6.1.1.1 Crypto-agility

Requirements on key lengths and algorithms must be changed over time to maintain an appropriate level of security. The SCMSMO shall monitor the need for such changes in the light of actual vulnerabilities and state-of- the-art cryptography. It will draft, approve and publish an update of this certificate policy if it decides that the cryptographic algorithms should be updated. Where a new issue of this CP signals a change of algorithm and/or key length, the SCMSMO will adopt a migration strategy, which includes transition periods during which old algorithms and key lengths must be supported.

In order to enable and facilitate the transfer to new algorithms and/ or key lengths, it is recommended that all PKI participants implement hardware and/or software that is capable of a changeover of key lengths and algorithms, and implement an update mechanism to adopt to new vulnerabilities or threats.

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 '2.1 Methods for the publication of certificate information'.

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. Private key protection and cryptographic module engineering controls

6.2.1. Cryptographic module standards and controls

The RootCA's private key is generated, stored, and used within a cryptographic module that meets the requirements of ISO/IEC 15408 Common Criteria Protection Profiles or FIPS 140-3 level 3, based on the results of a risk assessment and business requirements.

The ICA's private key shall be generated, stored, and used within a cryptographic module that meets the requirements of ISO/IEC 15408 Common Criteria Protection Profiles or FIPS 140-3 level 3, based on the results of a risk assessment and business requirements.

6.2.2. Private key (N out of M) multi-person 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. Private key escrow

Root CA's private key is not escrowed.

6.2.4. Backup of private keys

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 140-3 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. Destruction of 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 private key 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. Cryptographic module rating

Complies with the encryption module rating specified in '6.2.1 Cryptographic Module Standards and Controls'.

Uses cryptographic modules validated to FIPS 140-3 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 140-3 Level 3 and technical specifications of facilities and equipment of the authorized certification authority.

6.3. Activation data

Activation data refer to authentication factors required to operate cryptographic modules to prevent unauthorized access. The usage of the activation data of a SCMS model element cryptographic device shall require action by two authorized persons.

6.4. Computer security controls

The CAs' computer security controls is designed in accordance with the high security level by adhering to the requirements of ISO/IEC 27001.

6.5. Lifecycle technical 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.

6.6. Network security controls

The Root CA operates in isolation from public networks.

The Root CA's networks are hardened against attacks in accordance with the requirements and implementation guidance of ISO/IEC 27001.

The availability of the CA's networks is designed based on the estimated traffic.

6.7. Time stamping

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

7. Certificate profiles, CRL, CTL

7.1. Certificate profile

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. The AutoCrypt Root CA certificate profile is as follows.

```
{
  "version" : 3,
  "type" : "explicit",
  "issuer" : {
    "self" : "sha256"
  },
  "toBeSigned" : {
    "id" : {
      "name" : "rootca.v2x.autocrypt.io"
    },
    "cracaId" : "000000",
    "crlSeries" : 0,
    "validityPeriod" : {
      "start" :  Issuance Time : ,
      "duration" : {
        "years" : 30
      }
    },
    "appPermissions" : [
      {
        "psid" : 35,
        "ssp" : {
          "opaque" : "810002"
        }
      },
      {
        "psid" : 256,
        "ssp" : {
          "opaque" : "00010001010100"
        }
      }
    ],
    "certIssuePermissions" : [
      {
        "subjectPermissions" : {
          "all" : null
        },
        "minChainLength" : 3,
        "chainLengthRange" : -1,
        "eeType" : "(app(1), enrol(1), (0), (0), (0), (0), (0), (0))"
      },
      {
        "subjectPermissions" : {
          "explicit" : [
            {
```

```
            "psid" : 35
          }
        ]
      },
      "minChainLength" : 1,
      "chainLengthRange" : -1,
      "eeType" : "(app(1), enrol(1), (0), (0), (0), (0), (0), (0))"
    },
    {
      "subjectPermissions" : {
        "explicit" : [
          {
            "psid" : 38
          }
        ]
      },
      "minChainLength" : 1,
      "chainLengthRange" : -1,
      "eeType" : "(app(1), enrol(1), (0), (0), (0), (0), (0), (0))"
    },
    {
      "subjectPermissions" : {
        "explicit" : [
          {
            "psid" : 256,
            "sspRange" : {
              "all" : null
            }
          }
        ]
      },
      "minChainLength" : 1,
      "chainLengthRange" : -1,
      "eeType" : "(app(1), enrol(1), (0), (0), (0), (0), (0), (0))"
    }
  ],
  "verifyKeyIndicator" : {
    "verificationKey" : {
      "ecdsaNistP256" : {
        "compressed-y-0" : "Compressed Public Key"
      }
    }
  }
},
"signature" : {
  "ecdsaNistP256Signature" : {
    "rSig" : {
      "compressed-y-0" : "Signature Value r"
    },
    "sSig" : "Signature Value s"
  }
}
}
```

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 validity

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. Root CA

The Root CA certificate is a self-signed trust anchor with a maximum validity period of 30 years. In accordance with the pre-availability constraint, the Root CA certificate may be distributed no earlier than 12 months prior to the beginning of its validity period.

7.3. Certificate revocation list

This section describes the procedures for the issuance and publication of Certificate Revocation Lists (CRLs) by the CA or CRL Signer.

7.3.1. CRL Format and Profile Compliance

The Certificate Management Officer configures and manages the CA system to ensure that the CRLs generated strictly comply with the format and content requirements laid down in IEEE 1609.2.1.

The CRL profile is as follows.

```
{
        “version” : 1,
        “crlSeries” : 256,
        “crlCraca” : CRL Issuer Id,
        “issueDate” : Issuance Time,
        “nextCrl” : Next Issuance Time,
        “priorityInfo” : 1,
        “typeSpecific” : {
                “fullHashCrl” : {
                        “crlSerial” : a counter that increments by 1 every time,
                        “entries” : Sequence of Hash Based Revocation Info
                }
        }
}
```

7.3.2. Issuance Frequency and Validity Period

The System Administrator configures the automated scheduler of the CA system to issue the CRL at least annually.

7.4. Certificate trust list

Not applicable

8. Compliance audit and other assessments

8.1. Topics covered by auditor and audit basis

AutoCrypt undergoes periodic compliance audits to demonstrate conformity with this CPS.

A compliance audit is commissioned by the Root CA for itself. The audit report submitted as part of the Root CA inclusion process may be reviewed by the SCMS Manager and used to determine eligibility for inclusion.

An accredited PKI auditor performs the compliance audit at one or more of the following levels:

1. Assessment of the conformity of the Root CA's CPS with SCMS Manager's CP;

2. Assessment of the conformity of the Root CA's intended practices with its CPS prior to the start of operations;

3. Assessment of the conformity of the Root CA's actual operational practices with its CPS during ongoing operations.

The audit covers all processes described in the Root CA's CPS, including its facilities, systems, personnel, and operational controls.

The results of the compliance audit are provided to the Root CA and, where applicable, submitted to the SCMS Manager's CTL Committee in accordance with the SCMS governance procedures.

8.2. Frequency of the audits

AutoCrypt order a WebTrust compliance audit for themselves in the following cases:

(a) at their first setting-up (point in time audit)

(b) at every material change of the CP, if SCMS Manager requires it,

(c) every year during their operation.

8.3. Identity/qualifications of auditor

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

8.4. Auditor’s relationship to audited entity

Compliance audits of AutoCrypt V2X Root CAs are performed by a public accounting firm that is independent of the subject of the audit.

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

8.4.1. 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. Action taken as a result of deficiency

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. Communication of results

All evaluation results are reported to the SCMS Manager. 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 provisions

9.1. Fees

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. Financial responsibility

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. Confidentiality of business information

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 of personal information

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. Representations and warranties

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. Disclaimers of warranties

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. 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.

AutoCrypt's aggregate liability for direct damages verified to be caused by its negligence (excluding willful misconduct) shall be limited to the greater of the total fees paid to Autocrypt for the issuance of the relevant certificate or a strictly defined liability cap of $1000.

9.9. Indemnities

Relying parties are required to indemnify and hold AutoCrypt harmless from any damages arising from:

- Reliance on a certificate without validating its status (e.g., checking CRL).
- Reliance on or use of a certificate in violation of this CPS or the Relying Party Agreement.
- Damages resulting from reliance on an untrusted certificate (e.g., expired, revoked, or failed signature verification).

9.10. Term and Termination

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 '1.5.2 CPS approval procedures'.

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. Individual notices and communications with participants

The contact information for notifications or inquiries is as follows.

- Department: AutoCrypt V2X PKI Root CA Security Certification Center
- Phone Number: +82-2-2125-4000
- Address: (07241) 6F Sewoo Building, 115 Yeouigongwon-ro, Yeongdeungpo-gu, Seoul, South Korea
- E-mail: rootca@autocrypt.io

9.12. Amendments

9.12.1. Revision procedure

Refer to the certification process and approval process in '1.5.2 CPS approval procedures'.

9.12.2. Announcement of revision

Refer to the certification process and approval process in '1.5.2 CPS approval procedures'.

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. Dispute resolution procedures

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

9.14. Governing law

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. Miscellaneous provisions

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. Force majeure

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).