SAESOL Tech Certification Practice Statement

1 Introduction

1.1 Overview

This document serves as the Certification Practices Statement (CPS) for SAESOL Tech, Inc. ("SAESOL Tech"), outlining the principles and procedures governing SAESOL Tech's certification services. The CPS applies to all entities that participate in or utilize these services.

As part of SAESOL Tech's certification framework, this CPS is one of several governing documents. Other key documents include both public and private records. Additionally, SAESOL Tech may issue supplementary certification practice statements, which are accessible to relevant users and relying parties.

Following the IETF PKIX RFC 3647 CP/CPS framework, this CPS is structured into nine sections that detail the security controls, policies, and procedures for SAESOL Tech's certificate. To maintain the RFC 3647 structure, section headings that do not apply are explicitly marked as "Not applicable" or "No stipulation.

Figure 0-1
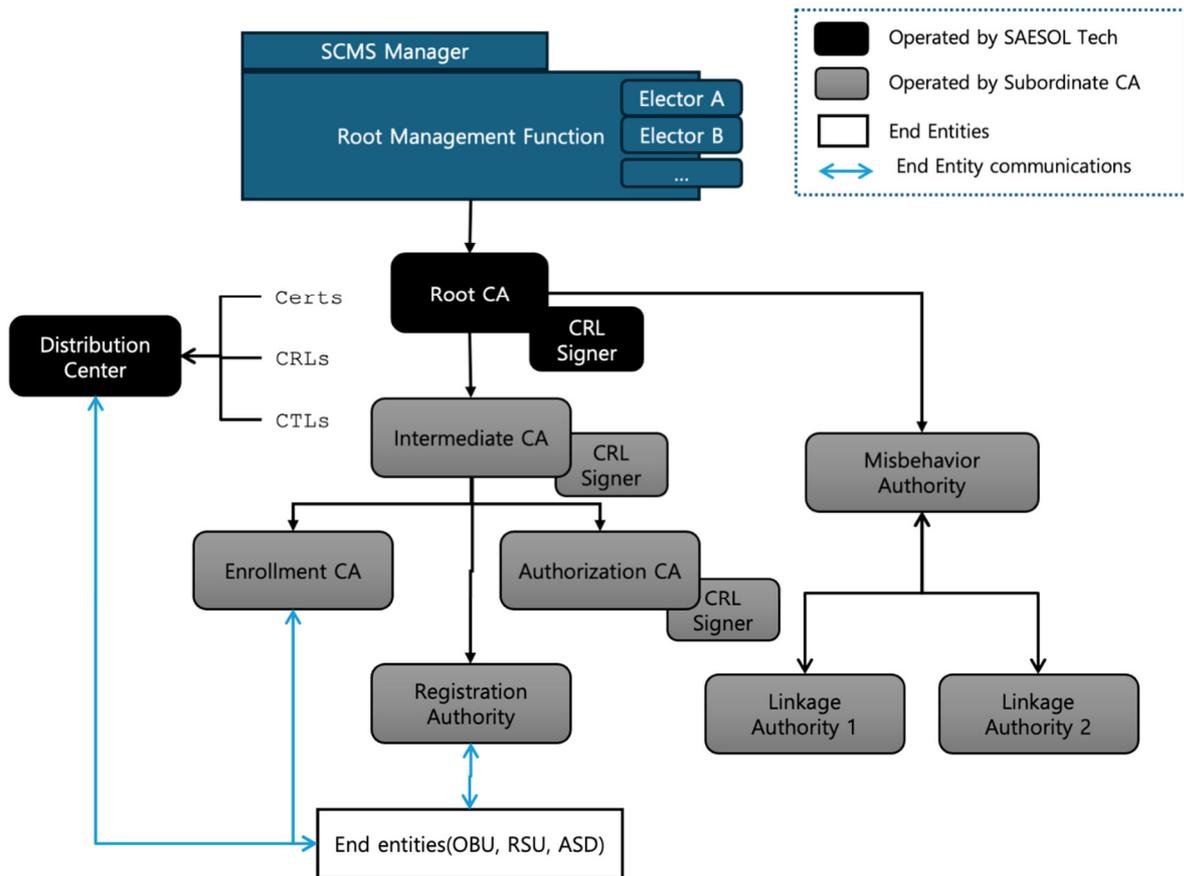
1.2 Document Name and Identification

This document describes the certificate practice of the SAESOL Tech V2X Root CA under the SCMS Manager's Certificate Policy. The following revisions were made to the original document:

Date	Changes	Version
2025-05-20	Initial Release	1.0.0
2025-05-28	DC name changed: dc.prod.v2x.saesol.tech -> dc.prod.s2x.io ICA name changed: ica.prod.v2x.s2x.io -> ica.prod.s2x.io	1.0.1

Date	Changes	Version
2025-06-12	**7.1.2** Intermediate CA Certificate Profile 'issuer.sha256AndDigest', 'toBeSigned.cracaId' is changed	1.0.2
2025-07-28	**1.6** remove unreferenced definitions and acronyms **6.2.5** Private Key Archival Accroding to the separate document about the policy of private key archival, the CA and SubCA private key should be archived. **2.1 - 2.4** Add PKI website as repositories. Explicitly refer the data in the repositories. **1.3.1, 1.3.2** the descriptions of the PKI Participants are changed. **3.2.1** add sentence that describe subCA should submit the evidence of the possession of domain if the certificate has domain name as id. 5.2.1 The following positions have been removed from the list of the Trusted Roles. - Policy Manager - Information Security Manager - HSM Token Holder - Safe Custodian	1.0.3

1.3 PKI Participants

1.3.1 SCMS Manager

The **SCMS Manager** is a consortium of stakeholders dedicated to the reliable and sustained operation of the **V2X ecosystem**. Its members include automotive OEMs, technology and service providers for vehicles, roadside infrastructure, and traffic management systems, as well as government agencies at the national, state, and local levels.

It is responsible for defining and maintaining **interoperability profiles, policies, procedures, and guidelines**, and conducts **research and development** to ensure the security and resilience of the ecosystem.

System components include **Electors, Root CAs, SCMS subsystems**, and **end entities**.

The SCMS Manager also performs regular **audits** to ensure participants remain compliant with its established best practices.

1.3.2 Electors

A component of the *Security Credential Management System (SCMS)* that manages trust of *root certificate authority (root CA)* certificates and peer *elector* certificates.

1.3.3 Accredited PKI Auditor

Accredited PKI Auditor is authorized for auditing SCMS Providers and Electors as stated in the Section 8:

1. audit the Electors and the SCMS Providers, which are operating Root CAs or a SubCAs.
2. receive the CPS of the Elector and the SCMS Provider,
3. is responsible to distribute the audit results to the CTL Committee for validation for inclusion of Elector or SCMS Providers' Root CA.

1.3.4 Certificate Authorities

The CPS addresses only SAESOL Tech V2X Root CA entity. Certification practices associated with subordinate certificate issuing entities in the CA hierarchy including Enrolment CAs and Authorization CAs, where applicable, are documented in one or more separate CPSs. SAESOL Tech V2X Root CA(s) are part of the certification path that issues certificates under a SAESOL Tech V2X Root CA trust domain. A trust domain may be part of a global SCMS V2X trust realm. Certification practices adhere to certification policies documented in the SCMS Manager's Certificate Policy. Root CA certificate profiles are consistent with Certificate Profiles specified by IEEE 1609.2 and IEEE1609.2.1.

The SAESOL Tech V2X Root CA is:

```
id: rootca.prod.s2x.io
issuer: self
```

1.3.4.1   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.

1.3.4.2   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.

1.3.4.3   Authorization CA(ACA)

A CA whose main responsibility is to issue authorization certificates.

1.3.4.4 CRL Signer

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

1.3.4.5 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).

1.3.4.6 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.

1.3.4.7 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.

1.3.4.8   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.

1.3.4.9   Distribution Center

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

```
https://dc.prod.s2x.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.

1.3.5 End Entities

The End Entities OBUs, RSUs or ASD(Aftermarket Safety Devices) which use certificates and relating keys to sign and/or encrypt messages for different applications

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The SAESOL Tech V2X Root CA issues certificates intended to secure V2X communications as specified by IEEE 1609.2, including DSRC and/or Cellular V2X communications. 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 Prohibited Certificate Uses

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

- circumstances that offend, breach or contravene any applicable law, regulation, decree or government order,
- circumstances that breach, contravene or infringe the rights of others,
- breach of this CPS or the relevant subscriber agreement,
- 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),
- circumstances that are inconsistent with the overarching objectives of improving road safety and promoting more efficient road transport.

1.5 Policy Administration

1.5.1 Organization Administrating the Document

The SAESOL Tech V2X Root CA PA approves this CPS and related operational documents and legal agreements.

1.5.2 Contact Person

Communications regarding CA policies and certification practices should be sent to the PA by registered mail or electronic mail to v2x.pa@saesol.tech

1.5.3 Person Determining CPS Suitability for the Policy

Members of the Policy Authority are listed in the internal SAESOL Tech V2X Root CA organizational roster and also included in the v2x.pa@saesol.tech mailing list.

The SAESOL Tech V2X PA is responsible for determining the suitability of policies illustrated within this CPS. The SAESOL Tech V2X PA is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition.

1.5.4 CPS Approval Procedures

The SAESOL Tech V2X PA reviews operational status at least annually and more frequently if required to review change requests to this CPS or other relevant CPSs. The update process is managed by the PA in consultation with Subscribers and other stakeholders. External change requests shall be submitted to the SAESOL Tech V2X Policy Authority (PA) via email. Internal change requests shall follow the SAESOL Tech V2X Root CA Change Request Process. In cases where the change is deemed significant or has the potential to impact PKI Participants, the request shall be subject to review and approval by the PA prior to implementation and dissemination.

1.6 Definitions and Acronyms

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

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.

canonical identifier(ID): 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).

certificate trust list (CTL): A list of the Electors and the root certificate authorities (Root CAs) that are trusted by a particular Security Credential Management System (SCMS) Manager, signed by the eligible Electors.

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

device configuration manager (DCM): A component of the Security Credential Management System (SCMS) that is responsible for bootstrapping an end entity (EE) and providing secure connection between the EE and the enrollment certificate authority (ECA).

distribution center (DC): A component of the Security Credential Management System (SCMS) that distributes public information such as certificates and certificate revocation lists. Contrast: registration authority (RA).

elector: A component of the Security Credential Management System (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).

enrollment certificate: A certificate that is used to request authorization certificates and to manage other interactions between an end entity (EE) and the Security Credential Management System (SCMS). Contrast: authorization certificate.

enrollment certificate authority (ECA): A certificate authority (CA) that issues enrollment certificates.

fully qualified distinguished name(FQDN): A **Fully Qualified Domain Name (FQDN)** is the complete domain name for a specific computer, host, or service on the internet. It includes both the hostname and the domain name, and it ends with a trailing dot representing the root of the DNS hierarchy (often omitted in practical usage). For example, `www.example.com`

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.

intermediate certificate authority (ICA): A certificate authority (CA) whose certificate was issued by another CA and whose main responsibility is to issue certificates to another CA, that is, an authorization certificate authority (ACA), an enrollment certificate authority (ECA), or another ICA.

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 of pseudonym certificates while preserving the privacy of an end entity (EE) against the authorization certificate authority (ACA).

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.

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.

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 end entity (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.

registration authority (RA): A component of the Security Credential Management System (SCMS) that is the main point of contact for an end entity (EE), and is responsible for provisioning the EE with authorization and successor enrollment certificates. Contrast: distribution center (DC), IEEE Registration Authority (IEEE RA).

root certificate authority (Root CA): A certificate authority (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 (SCMS) manager: A component of the Security Credential Management System (SCMS) whose role is to govern the entire SCMS, including defining and enforcing the certificate and security policies to be applied to Electors and Root CAs.

Subordinate Certificate Authority(SubCA): A **Subordinate CA** is a Certificate Authority that operates under the authority of a **Root Certificate Authority** (Root CA). It is issued a certificate by the Root CA (or another higher-level intermediate CA), allowing it to issue digital certificates to end entities such as servers, devices, or users.

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

Acronym or abbreviation	Meaning
ACPC	Activation Codes for Pseudonym Certificates
ACA	Authorization Certificate Authority
AES	Advanced Encryption Standard
API	Application Programming Interface
ASD	Aftermarket Safety Device
AT	Access Token
CA	Certificate Authority
CCF	Certificate Chain File
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
DNS	Domain Name System
ECA	Enrollment Certificate Authority
ECC	Elliptic Curve Cryptography
EE	End Entity
FQDN	Fully Qualified Domain name
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
ITS	Intelligent Transportation Systems
LA	Linkage Authority
MBR	MisBehavior Report

Acronym or abbreviation	Meaning
OBU	OnBoard 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
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
PSID	Provider Service Identifier
RA	Registration Authority
RFC	Request for Comments
RSU	RoadSide Unit
SCMS	Security Credential Management System
SSP	Service Specific Permissions
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
V2X	vehicle to everything

Table 0-1 Acronym or abbreviation

2 Publication and Repository Responsibilities

2.1   Repositories

The CA maintains a repository which is accessible to relevant PKI participants and other stakeholders at: distribution center `https://dc.prod.s2x.io` and SAESOL Tech V2X Root CA's PKI website `https://www.saesol.tech/certificateauthority`

2.2   Publication of Certification Information

The repository identified in Section 2.1 publishes the following information:

- A reference to the Certification Practices Statements
- The information listed in the Section 1.3.4.9   Distribution Center

The individual CRL, certificate, composite CRL-CTL, and CCF-CTL can be publicly accessed at:

```
CRL :
https://dc.prod.s2x.io/v3/crl?craca=49EA9FC96C6BA91A&crlSeries=256
Root CA Certificate :
https://dc.prod.s2x.io/v3/ca-certificate?certId=49EA9FC96C6BA91A
Composite-CRL-CTL :
https://dc.prod.s2x.io/v3/composite-crl-ctl?ctlSeriesId=FFFFFFFFFFFFFF00
CCF-CTL:
https://dc.prod.s2x.io/v3/ccf-ctl?ctlSeriesId=FFFFFFFFFFFFFF00
```

The CPS, RootCA certificate and individual CRLs can be accessed at :

```
https://www.saesol.tech/certificateauthority
```

2.3   Time or Frequency of Publication

SAESOL Tech publishes their newly issued CAs' certificates as it starts its operation via DC and RA. CRLs including composite-CRL-CTL are published within 24 hours after a status change via DC and RA. CCF-CTL are published within 6 hours after CCFs including other SCMS's and CTL are changed.

Certificate Practice Statements are published within 15 days after accepted modification from PA. Individual CRLs are also published at PKI website within 5 days after it is published by CRL signer. CA's certificates are also published at PKI website(https://www.saesol.tech/certificateauthority) within 5 days after it starts operating.

2.4   Access Controls on Repositories

The repositories are hosted within an access-controlled portal managed by SAESOL Tech, in accordance with the security policies of the SAESOL Tech V2X network platform. Updates can only be made by authorized SAESOL Tech portal administrators or programmatically by the CA. Portal administration secured using mutually authenticated HTTPS or SSH connections. CRL distribution points within the CA hierarchy are readable by PKI participants. Subscribers and other PKI participants can access other areas of repositories using credentials which are made when they sign up.

3 Identification and Authentication

3.1   Naming

3.1.1 Type of Names

The CertificateId attribute of type name in the certificate is in accordance with IEEE 1609.2.1.

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.prod.s2x.io
```

3.1.1.2   Names for ICA

The submitted CA name must be verified by the SAESOL Tech V2X Root CA to ensure that it does not conflict with any other existing names.

```
ica.prod.s2x.io
```

3.1.1.3   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 or Pseudonymity of Subscribers

An authorization certificate does 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

See section 3.1.1.

3.1.5 Uniqueness of Names

1. The Root CA, ICA, ACA, LA, MA names shall be unique.
2. The canonical IDs for End Entites 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 Recognition, Authentication, and Role of Trademarks

The SAESOL Tech V2X Root CA validates Subscriber corporate identities and FQDNs used in certificate names during the license application process to ensure that Subscribers are eligible to use any trademark protected names in applicable certificate subjects.

3.2   Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Root CA and ICA certificate requests are received from and processed by trusted personnel. Root CA/ICA issuance processes verify the signature on the request to determine the requestor has possession of the private key correspond to the public key in the certificate request.

An out of band hash fingerprint is used to validate external certificate requests.

The following table shows which actor is relevant for checking the key ownership of each actor.

Key owner	The actor responsible for the verification	Comments
Root CA	SCMS Manager organization	self-signed IEEE1609.2 certificate
ICA	Root CA	
ECA	ICA	
RA	ICA	
ACA	ICA	
LA	ICA	
MA	ICA	
CRL-Signer	corresponding CA such as RootCA, ICA or ACA	
DC	ICA	

If a domain URL is used as an ID value in a certificate, proof of domain ownership must also be submitted.

3.2.2 Authentication of Organization Identity

3.2.2.1 Authentication of SubCAs Organization Identity

The SAESOL Tech V2X Root CA check the identity of the organization and other registration information provided by certificate applicants for ICA certificates.

The SAESOL Tech V2X Root CA checks following.

- determine that the organization exists by using at least one third party identity proofing service or database, or, alternatively, organizational documentation issued by or filed with the relevant government agency or recognized authority that confirms the existence of the organization,
- require the certificate applicant to confirm certain information about the organization, that it has authorized the certificate application and that the person submitting the application on behalf of the applicant is authorized to do so. Where a certificate includes the name of an individual as an authorized representative of the organization, it shall also confirm that it employs that individual and has authorized him/her to act on its behalf.

3.2.3 Authentication of Individual Identity

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 Root or Intermediate CAs 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

SAESOL Tech Root V2X CA implementation are fully compliant with the IEEE1609.2.1.

SAESOL Tech participates in private and industry events hosted to demonstrate certificate functionality

on commercial V2X devices and interoperability with other SCMS component providers. Also SAESOL Tech participate the working group in SCMS Manager organization as a SCMS Manager member to validate the updated policy and the new standards to interoperable with other participants.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

3.3.1.1 ICA, ECA, RA, ACA, LA, MA, CRL signer, DC Certificate Renewal or Re-keying

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

3.3.1.2 End Entity's 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 key pair 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 possession of the new private key. 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 Entity's Authorization Credentials

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

3.3.2.1 CA Certificates

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

3.3.2.2 End Entities Certificates

The authentication of an end entity for enrollment or authorization certificate re-keying after revocation is 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,

- 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

Validation of Authority of an authorized requestor as documented in Section 3.4.1

3.4.3 End Entity Enrollment Certificates and Authorization

Request to revoke an EE enrollment certificate and authorization certificate can be originating from the EE subscriber or MA. Both of them shall authenticate themselves

4 Certificate Life-Cycle 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 by accredited 3rd party auditor, Root CA apply for insertion of its certificate in the CTL.

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

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

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

The Root CA addition to the CTL is an SCMS Manager Organization defined internal process, processed by the Ecosystem Audit Committee(EAC).

4.1.2.2   ICAs

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

Before an Intermediate Certificate Authority (ICA) is allowed to participate in the SAESOL Tech V2X PKI, the ICA must complete a formal enrollment process. This process includes the following steps:

1. Contractual Agreement : The ICA entity must have an established contractual agreement with the Root CA service, particularly if the ICA is owned or operated by a different entity than the Root CA.
2. Submission of Certificate Request : The ICA must generate a Certificate Signing Request (CSR) in accordance with the defined profile and cryptographic standards. The request must be securely transmitted to the Root CA.
3. 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.
4. 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.

Once enrolled, the ICA holds the following responsibilities within the SAESOL Tech V2X PKI:

1. Compliance with Policies: The ICA shall operate in strict adherence to the CPS, and all applicable security and operational guidelines established by the Root CA.
2. Certificate Lifecycle Management: The ICA is responsible for issuing, revoking, and managing certificates under its scope, ensuring their validity, and handling key rollover procedures as necessary.
3. Audit and Reporting: The ICA must maintain audit logs of all certificate-related activities and submit periodic compliance reports to the Policy Authority or Root CA as required.
4. Incident Response: In the event of a security incident, compromise, or non-compliance, the ICA must notify the Root CA immediately and follow the defined incident response procedures.
5. System Security: The ICA must ensure that its infrastructure, private keys, and certificate repositories are protected using approved cryptographic and physical security measures.

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 an entity different than the entity that owns the ICA, before issuing a SubCA or other SCMS elements certificate request, the SubCA's or other SCMS elements 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.

The EE subscriber can use multiple methods of authorization described in Section 1.3.4.2   Enrollment CA(ECA)

The EE may generate an enrollment certificate key pair and creates 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. Permissions for governmental use 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 of its certificates with a particular set of permissions. Special-purpose vehicles (such as police cars and other special-purpose vehicles with specific rights) may be enrolled at an additional Enrollment CA or have one additional enrollment for authorizations 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 SubCAs issuing certificates for such special-purpose EEs shall determine how the enrollment process applies to such EEs.

If the EE is in the process of migrating from one Enrollment CA to another Enrollment CA, the EE may be enrolled at two Enrollment CAs.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 Identification and Authentication of Root CA

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

The SCMS Manager Organization confirm its approval of the application to the Root CA. The Root CA send its self-signed certificate to the SCMS Manager Organization, which can be added to the CTL.

4.2.1.2 Identification and Authentication of ICA

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

The SAESOL Tech V2X Root CA authenticate an ICA certificate application using documents supplied by the applicant according to section 3 to validate the applicant's identity and authority.

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

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

The ICA authenticate an ECA, RA, ACA, LA, MA, DC certificate application using documents supplied by the applicant according to section 3 to validate the applicant's identity and authority.

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 should confirm the successful approval of the application to the respective CRL Signer. The CRL Signer should then submit a certificate request to the CRACA, which issues the certificate accordingly.

4.2.1.5   Identification and Authentication of EE Subscriber

The ECA is responsible for authenticating the EE subscriber. The Enrollment CA shall describe in its CPS the processes for EE subscriber authentication.

The ECA authenticate an EE subscriber's certificate application using documents supplied by the applicant according to section 3 to validate the applicant's identity and authority.

4.2.1.6   Identification and Authentication of EE

During enrollment certificate requests, in accordance with IEEE 1609.2.1, the ECA should use at least one of the authentication options mentioned in Section 1.3.4.2   Enrollment CA(ECA)

During successor enrollment certificate requests and successor enrollment certificate downloads, in accordance with IEEE 1609.2.1, the RA shall use at least one of the authentication options for both EE and RA mentioned in Section 1.3.4.7   Registration Authority (RA)

During authorization certificate requests and authorization certificate downloads, in accordance with IEEE 1609.2.1, the RA shall verify the EE's enrollment certificate and authenticate the ECA from which the EE received its enrollment certificate. If the RA is not able to authenticate the EE and ECA, the request shall be rejected. The RA shall use at least one of the authentication options for both EE and RA mentioned in Section 1.3.4.7   Registration Authority (RA).

During misbehavior report submission, in accordance with IEEE 1609.2.1, the RA should use at least one of the authentication options mentioned in Section 1.3.4.7   Registration Authority (RA)

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 Approval or Rejection of Root CA Certificates.

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

4.2.2.2 Approval or Rejection of ICA, ECA, RA, ACA, LA, MA, DC Certificates

The CA verifies SubCA certificate requests under its trust domain, inspecting relevant Subscriber qualifications and audit reports. If the check of an application is validated, the CA issues the requested certificate, otherwise the request is rejected and no certificate is issued.

4.2.2.3 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 positive result, the CRACA may issue a certificate to the requesting entity.

4.2.3 Time to Process Certificate Applications

4.2.3.1 ROOT CA/ ICA Certificate Application

The RCA or ICA processes certificate applications within 30 business days after a Subscriber Agreement has been signed and all documentation and authorizations concerning the application have been received. Such authorizations should include nominations and contact details for at least two duly authorized entity representatives who are authorized to act on behalf of the applicant organization.

4.2.3.2 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 7 business 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 should 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 issue its own self-signed Root CA certificate in IEEE 1609.2.1 format and send it to the SCMS Manager Organization for publication on the CTL.

The SCMS Manager Organization's CTL Committee check the audit results and the CPS of the Root CA, before it includes the Root CA on the CTL.

The SCMS Manager Organization makes the root certificate available via CTL at PUB.

4.3.1.2 ICA Certificate Issuance

The Root CAs issue ICA certificates in IEEE 1609.2 format.

The Root CA check the audit results of the ICA, before issues certificate for it.

The Root CA makes the ICA certificate available via RA repository or DC as soon as needed.

4.3.1.3   CRL Signer Certificate Issuance

The CRACA issue CRL Signer certificates in IEEE 1609.2 format.

The CRACA check the audit results of the CRL Signer, before issues certificate for it.

The CRACA makes the CRL Signer certificate available via RA repository or 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 issue ECA, RA, ACA, LA, MA, DC certificates in IEEE 1609.2 format.

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

The ICA 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 issues enrollment certificates in IEEE 1609.2.

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

4.3.1.6   Authorization Certificate Issuance

The ACA issues authorization certificates in IEEE 1609.2 format.

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

Authorization certificate requests and responses are encrypted to ensure confidentiality and signed to ensure authentication and integrity. End entities can receive the unencrypted responses, if they want.

4.3.2 Notification to Subscriber of Issuance of Certificates by the CA

Not applicable.

4.4 Certificate Acceptance

4.4.1 Conducting Constituting 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 end entity should verify the received enrollment certificates and authorization certificates against its original request, including the signature and the certificate chain. It shall discard all EC/AC responses that are not correctly verified. In such cases, it should send a new enrollment certificate / authorization certificate request.

4.4.2 Publication of the Certificate by the CA

Root CA certificates be made available to all participants through CTLs via the PUB of SCMS Manager Organization.

SubCAs' or other SCMS model elements certificates is published by the issuing CA.

Enrollment certificates and authorization certificates are not published.

ICA, ACA, and CRL Signer certificates can be published by the end entity via P2PCD according to IEEE 1609.2.1.

4.4.3 Notification of Certificate Issuance by the CA

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 Subscriber Private Key and Certificate Usage

4.5.1.1   Private Key and Certificate Usage for Root CA

The Root CA uses its Root CA private keys to sign its own (Root CA) certificates, CRLs, and SubCAs.

The Root CA certificate is used by PKI participants to verify the CRL and the SubCAs certificate.

4.5.1.2   Private Key and Certificate Usage for ICA

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

4.5.1.3   Private Key and Certificate Usage for ECA

The ECA uses its CA private keys to sign its own CSR and enrollment certificates.

ECA certificates are used by SCMS model elements and end entities to verify enrollment certificates and signatures from the ECA.

4.5.1.4   Private Key and Certificate Usage for RA

The RA uses its private keys to sign its own CSR and decrypt the encrypted PDUs. Also, this certificate can be used by the RA to authenticate itself in communication with other SCMS model elements and end entities.

RA certificates can be used by SCMS model elements and end entities to encrypt PDUs for the RA.

4.5.1.5　　　　Private Key and Certificate Usage for ACA

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

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

4.5.1.6　　　　Private Key and Certificate Usage for LA

The LA uses its private keys to sign its own CSR.

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

4.5.1.7　　　　Private Key and Certificate Usage for MA

The MA uses its private keys to sign its own CSRs and decrypt misbehavior reports.

MA certificates can be used by SCMS model elements to authenticate the MA in communication and to encrypt the key which is used to encrypt misbehavior reports.

4.5.1.8　　　　Private Key and Certificate Usage for CRACA and CRL Signer

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

CRACA and CRL Signer certificates are used by SCMS model elements and end entities to verify the CRLs.

4.5.2　Relying Party Public Key and Certificate Usage

Relying parties use the trusted certification path and associated public keys for the purposes referred to in the certificates and to authenticate the trusted common identity of enrollment certificates and authorization certificates.

4.6   Certificate Renewal

not allowed

4.6.1 Circumstance for Certificate Renewal

not applicable

4.6.2 Who May Request Renewal

not applicable

4.6.3 Processing Certificate Renewal Requests

not applicable

4.6.4 Notification of New Certificate Issuance to Subscriber

not applicable

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

not applicable

4.6.6 Publication of the Renewal Certificate by the CA

not applicable

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

not applicable

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

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

4.7.2 Who May Request Certification of a New Public Key

4.7.2.1 Root CA

The Root CA does not request re-key. The re-keying process is an internal process for Root CA, since its certificate is self-signed.

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

The SubCA's or other SCMS element's certificate re-keying request can be submitted in due time in order to be sure to have a new SubCA or other SCMS element certificate and operational SubCA or other SCMS element key pair before expiry of the current certificate. The date of submission must also take account of the time required for approval.

4.7.2.3 End Entity

The end entity can rekey its enrollment certificate according to IEEE 1609.2.1

4.7.3 Processing Certificate Re-Keying Requests

4.7.3.1   Root CA

Not Applicable

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

The SubCA or other SCMS element can request a new certificate or a rekey certificate as follows:

The SubCA or other SCMS element should 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 SubCA or other SCMS element should generate a new key pair and signs the request with the new private key (inner signature) to prove possession of the new private key. The whole request should be signed (oversigned) with the current valid private key (outer signature) to ensure the integrity and authenticity of the request.

4.7.3.3   End Entity

The end entity can rekey its enrollment certificate according to IEEE 1609.2.1.

4.7.4 Notification of New Certificate Issuance to Subscriber

Certificate issuance notification is treated as original certificate requests per Section 4.3.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Certificate acceptance is treated as original certificate requests per Section 4.4.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Certificate publication is treated as original certificate requests per Section 4.4.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Certificate notification is treated as original certificate requests per Section 4.4.

4.8   Certificate Modification

Not Allowed

4.8.1 Circumstance for Certificate Modification

Not Allowed

4.8.2 Who May Request Certificate Modification

Not Allowed

4.8.3 Processing Certificate Modification Requests

Not Allowed

4.8.4 Notification of New Certificate Issuance to Subscriber

Not Allowed

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not Allowed

4.8.6 Publication of the Modified Certificate by the CA

Not Allowed

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not Allowed

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

CA revokes a Certificate if one or more of the following occurs:

- The issuing CA (Root CA or SubCA) has reason to believe that the private key associated with the certificate has been compromised.
- An audit (see Section 8) results in a negative outcome.
- The SubCA or End Entity is no longer affiliated with, or managed by, the EE subscriber or the organization operating the SubCA.
- The certificate contains incorrect information that may lead to inappropriate use or reliance.
- The subscriber agreement has been terminated.
- A court or an entity with contractual or legal authority orders the revocation.

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

4.9.2 Who Can Request Revocation

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

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

The SubCA representative can request the revocation of its own SubCA 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 accept revocation requests from all authorized and authenticated parties.

CAs establish procedures that allow other entities to request certificate revocation for fraud or misuse. A 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 3 days notice to the subscriber and the SCMS Manager Organization, unless a shorter time period is necessary due to criticality.

Demonstrated key compression can be reported by anyone.

4.9.3 Procedure for Revocation Request

4.9.3.1   Removal of a Root CA

A Root CA should be removable from CTL. In the case of removal, the SCMS Manager Organization 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 Organization's CTL Committee, as defined in its internal processes.

The Root CA should immediately notify the SCMS Manager Organization of a known or suspected compromise of their private key.

4.9.3.2 Revocation of ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC Certificates

The Root CA process the revocation request – at normal conditions – in 5 days. If the revocation cause is the compromise of the key, this revocation is processed as soon as possible. Revoked certificates are published on a CRL within 24 hours.

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

The SubCA and the other SCMS element immediately notify the issuing CA of a known or suspected compromise of its private key.

Before revoking a Subordinate CA (SubCA) certificate upon request, the Root CA (or appropriate authority) must verify the authenticity and authorization of the entity submitting the revocation request.

The requestor must be an authorized representative of the SubCA entity or the Policy Authority (PA).

Verification may include:

- Digital signature validation using the SubCA's active private key
- Confirmation of identity through previously registered contact channels
- Out-of-band verification, if necessary (e.g., via phone or secure email)

Once authentication is complete and the revocation request is approved, the following steps shall be followed:

1. Initiation

The Root CA receives and validates the revocation request for the specified SubCA certificate.

2. Revocation Reason Logging

The reason for revocation (e.g., key compromise, cessation of operation, suspected misbehavior) must be recorded.

3. Update to Revocation Repository

The revoked SubCA certificate shall be added to the appropriate Certificate Revocation List (CRL), or registered in the revocation status database used in the V2X environment (e.g., misbehavior reporting system or CRACA structure).

4. Propagation of Revocation Status

The updated revocation status shall be distributed to all relevant SCMS entities, ensuring devices and relying parties are aware of the SubCA's revocation.

5. Audit Logging

All actions related to the revocation process (authentication, decision, timestamp, and propagation) shall be logged and retained for auditing purposes.

4.9.3.3 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 is not accepted for any usage.

The ECA processes the blocking/revocation request – at normal conditions – in 5 days. If the blocking/revocation cause is the compromise of the key, this revocation is processed as soon as possible.

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

4.9.3.4 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:

1. EE subscriber requests the revocation
2. EE subscriber termination,

3. MA requested it,

4. when a court decision orders,

The ACA processes the revocation request – at normal conditions – in 5 days. If the revocation cause is the compromise of the key, this revocation is 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 activation code is not received by the EE.

4.9.4 Revocation Request Grace Period

The CA consider any revocation requests which impact the security or integrity of the PKI within 1 business day. Other requests are considered within 5 business days.

4.9.5 Time Within Which CA Must Process the Revocation Request

The CA process a revocation request on or before its effective revocation date, which shall be no more than 1 business day for revocations which have a high potential to negatively impact the security or integrity of the PKI.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties' devices and application software must check relevant CRLs and certification paths prior to relying upon a certificate.

4.9.7 CRL Issuance Frequency

The CRL is published on a annual schedule and in all cases prior to the expiration of the current CRL. Each CRL is also issued no later than the 'nextCrl' time specified in the previously published CRL for the same scope.

4.9.8 Maximum Latency for CRLs

Maximum CRL latency is one business day.

4.9.9 On-Line Revocation/Status Checking Availability

The CA does not support any on-line revocation / certificate status checking such as Certificate Status Protocol (OCSP).

4.9.10   On-Line Revocation Checking Requirements

The CA does not support on-line certificate status protocol.

4.9.11   Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12   Special Requirements Re Key Compromise

The CA uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects that one of the CA's private keys has been compromised, publishing a CRL and communicating a mitigation plan which is developed based on the identified root cause of the compromise and the severity of the issue.

Analysis is performed for revocations to determine the cause of the compromise and whether there is reason to consider any mitigation actions.

4.9.13   Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.9.17 Processing of Misbehavior Reports

MA processes misbehavior reports only if the following requirements are fulfilled:

1. the signature of the reporting End Entity on the MBR is valid,
2. valid and relevant Elector certificates are available,
3. valid and relevant CRL and CTL are available,
4. the Root CA certificate and the ICA certificate of the MA certificate chain are valid,
5. on the relevant and valid CTL root certificate of the MA is listed.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Not applicable.

4.10.2   Service Availability

Not applicable.

4.10.3   Optional Features

Not applicable.

4.11 End of Subscription

Not applicable.

4.12 Key Escrow and Recovery

Not applicable.

4.12.1   Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2   Session key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

5.1.1.1 Root CA

The Root CA is securely installed at SAESOL Tech's facility in South Korea and operated offline. The secure facility is used for conducting Root keying ceremonies, and for Root issuance of certificates for online components of the PKI such as ICA, ECA, PCA, RA, LA, PG, CRLG and MA. The construction of the facility housing the CA equipment is consistent with facilities used to house high-value, sensitive information. Facility construction includes re-enforced doors, walls, ceilings, and floors. The site location and construction, when combined with other physical security protection mechanisms such as intrusion sensors, electronic access controls and video surveillance of the facility provides robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

Physical access to the CA secure facility is restricted to employees on the Permanent Authorized Access List and escorted visitors. Physical access controls on the facility include the following.

- Facility access requires fingerprint recognition and smart card to pass through electronic door locks. Door locks include remote monitoring, alarm, and dispatch of security personnel to address alarm events.
- Facility access requires dual person access to pass through physical door locks.
- Facility contains a safe requiring two combinations to open.
- Facility access points are under video surveillance.

- Facility is under video surveillance.
- Logs are kept of all access, including names and roles of escorted visitors.

The process for managing security incidents is described in the SAESOL Tech V2X Business Continuity Plan document.

5.1.3 Power and Air Conditioning

Smooth shutdown of the C-ITS trust model equipment in the event of a lack of power. These SCMS model elements facilities shall be equipped with heating/ventilation/air-conditioning systems to maintain the temperature and relative humidity of the SCMS model element's equipment within operational range.

5.1.4 Water Exposures

CA equipment and media is installed so that it is not in danger of water exposure.

5.1.5 Fire Prevention and Protection

The facilities that house the CA are constructed and equipped, and procedures implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures meet all local applicable safety regulations.

5.1.6 Media Storage

Media related to the operation of the CA is stored in two locations.

- A copy of root keying material and activation data is securely stored within a safe within the facility and cryptographically secured. Activation tokens are stored in key safes and inactive removeable media are stored in a safe in tamper evident containers.
- A copy of all CA data is retained in off-site backup facilities. All CA keying material or sensitive data stored off-site is cryptographically secured and integrity protected.

5.1.7 Waste Disposal

All waste including paper, media or any other waste is destroyed in secure and irreversible method 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, are destroyed before being released for disposal.

5.1.8 Off-Site Backup

A full backup of CA software and data including a backup of keying material is created for DR operation.

The database and HSM of the Root CA / ICA is backed up after every successful key ceremony and root or ICA signing operation. This backup is then transferred to the backup storage facility and logged into a Disaster Recovery Backup Log.

5.2 Procedural Controls

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

5.2.1 Trusted Roles

5.2.1.1 Executive Director

The Executive Director responsible for approving certification practice statements as well as key strategies and plans plays a critical role in the governance of the certification authority. They review and authorize policy documents to ensure alignment with legal, regulatory, and organizational requirements. In addition, they provide strategic oversight, make high-level decisions regarding operational planning, and ensure that the certification authority's objectives are met in a secure and efficient manner.

5.2.1.2 Technical Operations Manager

The Technical Operations Manager provides management oversight of all technical operations. This role ensures maintenance of critical systems and may involve assisting the IT Configuration Administrator.

5.2.1.3 Internal Auditor

The Internal Auditor is responsible for reviewing the audit logs and performing or overseeing internal compliance audits to ensure that the CA and associated administrative applications are operating in accordance with the SAESOL Tech CPS.

5.2.1.4 IT Configuration Administrator

The IT Configuration Administrator is responsible for installing and configuring system hardware and software, and for updating the CA software and performing system maintenance.

5.2.1.5 Software Administrator

Management of the Root CA certificate system (software) and the lifecycle of the Root CA certificate, including its generation, revocation, and other related operations.

5.2.1.6 Root CA HSM Administrator

Management of the Root CA HSM device and the lifecycle of cryptographic keys, including key pair generation, usage, and destruction.

5.2.1.7 System Developer

Responsible for the design, implementation, and maintenance of PKI components, including certificate issuance, revocation, cryptographic protocol integration, and secure storage.

5.2.2 Number of Persons Required per Task

Internal control procedures are designed to ensure that at a minimum, two trusted persons are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons, with a minimum of at least three HSM token holders required to create or activate a key. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device.

5.2.3 Identification and Authentication for Each Role

Personnel fulfilling trusted roles are screened by SAESOL Tech hiring practices.

Trusted role personnel are given requisite system logons, access to secure facilities and smart cards for HSM access as befits their roles and responsibilities in the CA.

All personnel fulfilling a trusted role are identified on the SAESOL Tech Root V2X CA Operations Responsibility Matrix.

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 SAESOL Tech V2X Root CA Operations Responsibility Matrix and CA keying ceremonies documentation.

A person can fulfill multiple roles as described in section 5.2.1, except in cases when two persons of the same role are required for a procedure, an individual can only act as one person of that role. For example, if a procedure calls for two HSM token holders, a single person cannot act as both.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Trusted roles and responsibilities, as specified in the CPS, are documented in job descriptions and clearly identified. PKI personnel have job descriptions defined to ensure separation of duties and least privilege, and position sensitivity is determined based on the duties and access levels, background screening and employee training and awareness.

All CA personnel are subject to SAESOL Tech HR policies and terms of employment.

Personnel undergo annual security training.

5.3.2 Background Check Procedures

Background investigation and the hiring process follow SAESOL Tech standard procedures for employee screening, as described in the document Background Screening Guidelines, which is maintained by SAESOL Tech Human Resources (HR) team and by the CA's Personnel Hiring and Disciplinary Procedure documents.

Checks completed for all external hires include the following:

- Validation of previous five year of employment history, if applicable.
- Validation of highest level of education attended and/or required for the position.
- Validation of professional certification.

5.3.3 Training Requirements

Training programs are reviewed periodically, and their training address matters that are relevant to functions performed by their personnel.

Training programs include the stuff that are relevant to the particular environment of the trainee,

including:

- security principles and mechanisms of the SCMS model elements,
- all duties the person is expected to perform, and internal and external reporting processes and sequences,
- PKI business processes and workflows,
- incident and compromise reporting and handling,
- disaster recovery and business continuity procedures,
- configuration and access management of the PKI system,
- sufficient IT knowledge.

5.3.4 Retraining Frequency and Requirements

All CA personnel are trained to correctly operate all CA software and hardware relevant to their roles. CA personnel shall be re-trained whenever the Policy Authority or the CA Operations Manager determines that a significant change has been made to the software, hardware, SCMS Manager's certificate policies, or the SAESOL Tech V2X Root CA policies and procedures.

5.3.5 Job Rotation Frequency and Sequence

Any change in roles in the administration or operation of trust model elements is accompanied by a change of account access and smart card privileges where relevant, authorized and documented by an approved work order and publication of a revised list of trusted role personnel.

5.3.6 Sanctions for Unauthorized Actions

Disciplinary action is taken whenever it is determined that a CA employee has violated the CA procedures, or has acted in a manner detrimental to the CA objectives, such that actual or apparent compromise of security and integrity is possible.

Actions do not have to be intentional to result in disciplinary action.

The employee's immediate supervisor or Root CA operation manager normally assesses the need for disciplinary action. HR may assist in the implementation of any disciplinary actions.

Employees are given formal documentation of the violation.

If dismissed from a role, the employee's CA access credentials are removed.

5.3.7 Independent Contractor Requirements

Independent contractors fulfilling permanent trusted roles shall be treated in role qualification and assignment as ordinary employees. Other contractors or personnel acting in a non-trusted role or temporary capacity (e.g. maintenance technician, auditor) shall be escorted and supervised when accessing dedicated PKI equipment with their presence authorized in approved work PKI orders and logged in authorized visitor logs.

5.3.8 Documentation Supplied to Personnel

CA personnel are provided copies of this CPS, all CA Operations policies and procedures relevant to their trusted role, and all CA Operating Manuals. Specialist administrators and technicians may have access to design documentation or software to facilitate a deeper understanding of underlying PKI system behavior.

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):

- Type of event
- Date and time the event occurred.
- Result of the event: success or failure where appropriate.
- Identity of the entity and/or operator that caused the event if applicable.
- Identity of the entity for which the event is addressed.

Detailed list of the audit logs is listed below.

- physical facility access – access by physical persons to the facilities shall be recorded. An event shall be created every time a record is created,
- 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,
- logical access – an event shall be generated when an entity (e.g. a program) has access to sensitive areas (i.e. networks and servers),
- backup management – an event shall be created every time a backup is completed, either successfully or unsuccessfully,
- log management – logs shall be stored. An event shall be created when the log size exceeds a specific

size,

- 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,

- 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,

- manufacturer registration – an event shall be created when a manufacturer is registered,

- end entity events -– an event shall be created when an end entity is registered and every time when registration status is changed/updated,

- HSM management – an event shall be created when an HSM security breach is recorded,

- 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,

- security management (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).

5.4.2 Frequency of Processing Log

Event logs are reviewed as part of periodic internal audits. Audit logs are reviewed in response to alerts based on irregularities and incidents within the CA.

Audit log processing consists of a review of the audit logs and documenting the reason for all significant events in an audit log summary. Audit log reviews 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 is documented.

The audit log will be archived at least quarterly. 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 quarter.

5.4.3 Retention Period for Audit Log

Log records relating to certificate life cycles are kept for at least 5 years after the corresponding certificate expires.

5.4.4 Protection of Audit Log

Audit logging information generated by the CA is integrity protected by the CA software. Audit logs are electronically archived and retained in a secure SAESOL Tech repository as part of the CA records archive.

The integrity and confidentiality of the audit log is guaranteed by a role-based access control mechanism. Internal audit logs can be accessed only by personnel holding trusted roles with the proper authorization. Access is only granted with multi-factor authentication. It is technically ensured that users cannot access their own log files.

Electronic audit log entries are signed with a secure method.

5.4.5 Audit Log Backup Procedures

Electronic audit logs follow the backup described in section 5.1.8.

5.4.6 Audit Collection System (Internal or External)

The audit log collection system is internal to the CA software and hardware. Automated audit processes are invoked at system and application startup, and cease during system shutdown.

5.4.7 Notification to Event-Causing Subject

Audit log events record, where applicable, the associated trusted role or trusted person(s) as one of the event details.

5.4.8 Vulnerability Assessment

The SAESOL Tech V2X Root CA Operations Team will perform routine self-assessment of security controls as described in the Risk Assessment and Mitigation Strategy document.

5.5   Records Archival

5.5.1 Types of Record Archiving

CA records shall be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including revoked or expired certificates) issued by the CA. At a minimum, the following data shall be backed up:

- PKI Operations and Event Logs
- Certification Practices Statement documents
- Other agreements concerning operations of the CA
- All certificates issued and/or published
- Audit log data (as described in section 5.4.1)
- Subscriber identity authentication data
- Subscriber agreements or EULAs, if applicable
- Enrollment forms & verification evidence
- All CRLs issued and/or published
- Documentation required by compliance auditors

5.5.2 Retention Period for Archive

The SAESOL Tech V2X Root CA retains certificate records and related documentation (see Section 5.5.1) for five (5) years from the date of expiration or, in the case of revoked certificates, from the date of revocation, unless otherwise specified in a valid business agreement.

5.5.3 Protection of Archive

Archive records are stored in a secure USB storage in a manner that prevents unauthorized modification or destruction. The contents of the archive shall not be deleted except with approval of the PA or as required by law.

The integrity and confidentiality of the audit archive is guaranteed by a role-based access control mechanism. Internal audit archive can be accessed only by personnel holding trusted roles with the proper authorization. It is technically ensured that users cannot access their own archive files.

5.5.4 Archive and Backup Procedures

Offline trust model elements are incrementally backed up after keying ceremonies with full backups at least annually.

5.5.5 Requirements for Time-Stamping of Records

The system time on an offline trust element must be verified and manually adjusted if necessary prior to operating the CA using the time source referencing a reliable carrier network.

5.5.6 Archive Collection System (Internal or External)

Not applicable.

5.5.7 Procedures to Obtain and Verify Archive Information

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

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

5.6   Key Changeover

CA public key changes are carried out periodically with prior announcement, ensuring minimal disruption to relying parties and dependent systems.

SubCA or other SCMS model elements shall generate new key pairs and request a new certificate before

expiration of their current valid certificate. The validity period of the new Sub-CA or other SCMS model elements certificate shall start prior to the planned deletion of the current private keys. The SubCA or other SCMS model elements shall take care that the new certificate is distributed to relevant subscribers and relying parties before the start of its validity period. The SCMS model element shall activate the new private key when the corresponding certificate becomes valid.

5.7 Compromise and Disaster Recovery

The following describes the general principles applied to all CAs:

- The CA and supporting trust elements are deployed in accordance with SAESOL Tech operational requirements for high availability requirements for critical customer facing services.
- The CA implements processes and procedures described in the SAESOL Tech V2X Root CA Disaster Recovery and Business Continuity Plan (DRBCP).

5.7.1 Incident and Compromise Handling Procedures

If personnel responsible for the management of the RCA/ICA detect or receive a report of a potential hacking attempt or other form of compromise, they perform an investigation to determine the nature and the degree of damage. The scope of potential damage is assessed by the personnel responsible for the management of the CA entity to determine if the PKI component needs to be rebuilt, if only some certificates need to be revoked, and/or if the PKI component has been compromised.

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 SAESOL Tech CA Operation Manager is called in to determine root cause and possible damage.

SAESOL 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 (DRBCP) 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 Computing Resources, Software, and/or Data Are Corrupted

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.

5.7.3 Entity Private Key Compromise Procedures

In case of a CA key compromise, the PA shall be notified within 24 hours of the discovery or suspicion of a key compromise event. Subsequently, the CA installation shall be reestablished. If the CA distributes a trusted certificate for use as a trust anchor, the new self-signed certificate must be distributed via the standard secure out-of-band mechanisms.

Subscribers shall be notified but subscriber certificates will not be renewed automatically by the CA under the new key pair. The CA will require subscribers to repeat the initial certificate application process.

Relying parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operation with new certificates.

5.7.4 Business Continuity Capabilities After a Disaster

SAESOL Tech maintains data center and disaster recovery facilities. After a disaster SAESOL Tech will execute its Disaster Recovery and Business Continuity Plan (DRBCP) to resume operations from this location until a primary operations site can be restored. CA personnel will be able to securely activate CA private keys using m-of-n (3 of 5) split key shares in DR facilities to recover core CA operations

5.8   CA or RA Termination

As soon as possible prior to termination, the CA advises all other organizations to which it has issued certificates of its termination plans and, where applicable, assign subscriber licenses and transfer relevant PKI data and archives to an authorized assignee. In the event of the termination of the CA service without assignment, the CA shall:

- Provide subscribers/licensees, legal and applicable regulatory authorities notice of termination
- Stop issuing certificates with validity periods beyond the proposed termination or suspension date
- On termination date, in the case of a terminated SubCA, the superior CA shall revoke the SubCA and issue a new CRL with the list of revoked SubCAs. In the case of a root CA the corresponding CA shall revoke itself by issuing a CRL containing itself.
- Communicate last revocation status information (CRL signed by root CA) to the relying party indicating clearly that it is the latest revocation information.
- Destroy the CA private key.
- Archive all audit logs and other records prior to termination and if applicable transfer to an appropriate authority.

Archived records are transferred to an entity designated by the PA. In the event of the termination of the CA services, SAESOL Tech will be responsible for keeping all relevant records regarding the needs of CA and PKI components. The requirements of this article may be varied by license agreement to the extent that such modifications affect only the contracting or licensed parties.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information is generated in HSMs which have been NIST validated to FIPS 140-3 Level 3. CA keys are generated in auditable keying ceremonies as document by CA key ceremony procedures. Public keys are published for relying parties. The CA does not generate Subscriber key pairs.

6.1.1.1 Cryptographic Requirements

	ecdsaBrainpoolP256r1WithSha256	ecdsaBrainpoolP384r1WithSha384	ecdsaNistP256WithSha256	ecdsaNistP384WithSha384
Root CA	signature/verification	signature/verification	signature/verification	signature/verification
ICA	signature/verification	signature/verification	signature/verification	signature/verification
ECA	signature/verification	signature/verification	signature/verification	signature/verification
ACA	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption
CRL Signer	signature/verification	signature/verification	signature/verification	signature/verification

	ecdsaBrainpoolP256r1WithSha256	ecdsaBrainpoolP384r1WithSha384	ecdsaNistP256WithSha256	ecdsaNistP384WithSha384
RA	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption
LA	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption
MA	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption
DC	signature/verification	signature/verification	signature/verification	signature/verification
EC	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption
AC	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption	signature/verification encryption/decryption

6.1.1.2   Crypto-Agility

Requirements on key lengths and algorithms change over time to maintain an appropriate level of security. The SCMS Manager Organization guides and manages such changes in the light of actual vulnerabilities and state-of-the-art cryptography. It drafts, approves and publishes an update of the CPS when cryptographic algorithms need to be updated. Where a new version of the CP signals a change in algorithm and/or key length, the SCMS Manager Organization implements a migration strategy, including

transition periods during which legacy algorithms and key lengths remain supported.

The structure and operation of the Root CA are designed to reflect and comply with the requirements specified in the CPS to the greatest extent possible.

To enable and facilitate the transition to new algorithms and/or key lengths, all PKI participants including Root CA and ICA implement hardware and/or software capable of supporting key lengths and algorithms changes and maintain update mechanism to respond to new vulnerabilities or new threats.

6.1.2 Private Key Delivery to Subscriber

The CA does not directly provide private key material to Subscribers. Instead, any implicit private key information is always encrypted during transmission and is also stored in encrypted form, following the IEEE 1609.2 specifications.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys generated by Subscribers are sent to CA entities using IEEE 1609.2 specified protocols which enable the CA to validate possession of the private key. Certificate requests are transmitted over secure, authenticated links or validated using out-of-band fingerprint techniques when requests are transmitted via email

6.1.4 CA Public Key Delivery to Relying Parties

The CA and SubCA certificates, where applicable, are published as described in section 2.2.

6.1.5 Key Sizes

The CA supports ECDSA with NIST P-256/SHA-256, ECDSA with NIST P-384/SHA-384, ECDSA with BrainPool-256/SHA-256 and ECDSA with BrainPool-384/SHA-384 signature algorithms for IEEE 1609.2 as specified in FIPS 186-4.

6.1.6 Public Key Parameters Generation and Quality Checking

The CA supports ECDSA as defined in FIPS 186-4 using FIPS certified cryptographic modules for CA key generation.

Certificate public keys are validated prior to certificate issuance following FIPS 186-4 specifications

6.1.7 Key Usage Purposes

Certificate key usage fields are set to adhere to specifications for CA entities as described in IEEE 1609.2 and IEEE1609.2.1 SCMS documentation and as described in the Certificate Profiles of this CPS.

Root CA certificate signing key usages are asserted as critical.

To elaborate further, the following two fields in the certificate can be used to infer the intended use of the certificate

- `appPermissions` indicates the permissions that the certificate holder has to *sign application data* with this certificate. A valid instance of appPermissions contains any particular Psid value in at most one entry.
- `certIssuePermissions` indicates the permissions that the certificate holder has to *sign certificates* with this certificate. A valid instance of this array contains no more than one entry whose subjectPermissions field indicates all. If the array has multiple entries and one entry has its subjectPermissions field indicate all, then the entry indicating all specifies the permissions for all PSIDs other than the ones explicitly specified in the other entries.

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 140-2 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

At least three out of the five HSM Token Holders are required to invoke the complete CA signature process or access any cryptographic module containing the CA private signing key. Manual access to the cryptographic module requires a two-factor authentication for the administrator.

For SubCAs, at least three token holders out of the five are required to activate the private key. Once activated, the SubCA private key can be used to sign certificate requests without further human interaction. Access to an activate SubCA private key is controlled using a passphrase.

CA signing keys are backed up under a minimum three-out-of-five person control scheme. Access to disaster recovery backups of CA signing keys requires the approval of at least three of five designated individuals. This list is available for compliance audit inspection.

6.2.3 Private Key Escrow

CA private keys are not escrowed.

6.2.4 Private Key Backup

CA Private Keys are generated inside a FIPS 140-3 Level 3 validated HSM. When deactivated these keys are encrypted and protected by multiple cryptographic tokens that enforce multiple person control described in section 6.2.2.

Backups of the private keys are created using techniques specified by the module manufacturer. A private key is always encrypted when it leaves the protection boundary of an HSM.

6.2.5 Private Key Archival

The archival policy for the CA and SubCA private keys, including conditions and retention requirements, is defined in a separate document SAESOL Tech Key Archival Procedure.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

A private key is transferred into or from an HSM using techniques specified by the module manufacturer using at least three-person control to reactivate the key as described in Entrust HSM Management document.

6.2.7 Private Key Storage on Cryptographic Module

See section 6.2.4

6.2.8 Method of Activating Private Key

Private keys stored in an HSM are activated using smart card keys according to techniques specified by the module manufacturer. To activate a key, at least three(3) trusted persons must present their smart card keys together with the associated passwords.

For the Root CA which are normally offline, activation is required every time the entity is activated for a

private key is generation or signing operation.

The CA maintains no involvement in the protection or distribution of Subscriber private keys.

6.2.9 Method of Deactivating Private Key

For the CA, the HSM is never left in an unlocked, unattended state or otherwise left open to unauthorized access. After use, the cryptographic module is deactivated as recommend by the manufacturer and documented in the Entrust HSM User Guide.

In practice, deactivating a private key on an Entrust HSM typically involves either removing the key from the HSM, revoking its access permissions, disabling or deleting the associated smartcard or OCS, or making the key file inaccessible.

6.2.10 Method of Destroying Private Key

CA private signing keys stored in HSMs are destroyed using the method offered by the cryptographic module.

All backups of the private keys are likewise destroyed so that the destroyed private key cannot be re-activated.

6.2.11 Cryptographic Module Rating

See section 6.2.1

6.3   Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CA retains copies of all CA entity public keys for archival in accordance with section 5.5 for at least five (5) years after any certificate based thereon ceases to be valid.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

All certificates and corresponding keying materials have maximum validity periods not exceeding those recommended by SCMS Manager and IEEE 1609.2 specifications.

CA private keys are allowed to be used starting from the beginning of their corresponding certificate's validity period. They are retired and prevented from signing new certificates at least 365 days before the certificate's expiration date to allow sufficient time for certificate re-keying and distribution.

The validity periods of certificates subject to this CPS is described in section 7.

6.4   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 elements cryptographic device shall require action by at least three out of the five authorized persons.

6.4.1 Activation Data Generation and Installation

no stipulation.

6.4.2 Activation Data Protection

no stipulation.

6.4.3 Other Aspects of Activation Data

no stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Control

The CA's life cycle technical controls are described in the following sub-sections.

6.6.1 System Development Controls

The SAESOL Tech V2X Root CA uses a formal configuration management methodology for installation and ongoing maintenance of any CA system. Any modifications or upgrades to the system are documented and

controlled.

6.6.2 Security Management Controls

The SAESOL Tech V2X Root CA configurations are periodically reviewed to identify any unauthorized changes. The SAESOL Tech V2X Root CA maintains change control mechanisms to document, control, monitor, and maintain the installation and configuration of the CA systems, including any modifications or upgrades. When loading software onto a CA system, SAESOL Tech V2X Root CA verifies that the software is the correct version and is supplied by the vendor free of any modifications.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7   Network Security Controls

The Root CA are operated in an isolated, normally off-line security facility. External certificate requests are scanned for malware in a secure staging area prior to processing. SubCA and on-line CA trust elements are protected by firewalls in dedicated secure datacenters which offer resilient, dedicated external network links. Internal SubCA or supporting trust element enrollment is handled through controlled processes between offline CA components and online ancillary CA systems (e.g., CRLG) or SubCA entities.

6.8   Time Stamping

See section 5.5.5.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profiles

7.1.1 Root CA Certificate Profile

```
{
  "version": 3,
  "type": "explicit",
  "issuer": {
    "self": "length(256bit)"
  },
  "toBeSigned": {
    "id": {
      "name": "rootca.prod.s2x.io"
    },
    "cracaId": "000000",
    "crlSeries": 0,
    "validityPeriod": {
      "start": issuance timestamp ,
      "duration": {
        "years": 30
      }
    },
    "appPermissions": [
      {
        "psid": 35,
        "ssp": {
          "opaque": "810002"
        }
```

```json
    },
    {
      "psid": 256,
      "ssp": {
        "opaque": "00010001010100"
      }
    }
  ],
  "certIssuePermissions": [
    {
      "subjectPermissions": {
        "all": null
      },
      "minChainLength": 3,
      "chainLengthRange": -1,
      "eeType": [
        "app",
        "enrol"
      ]
    },
    {
      "subjectPermissions": {
        "explicit": [
          {
            "psid": 35
          }
        ]
      },
      "minChainLength": 1,
      "chainLengthRange": -1,
      "eeType": [
        "app",
        "enrol"
      ]
```

```json
        },
        {
          "subjectPermissions": {
            "explicit": [
              {
                "psid": 38
              }
            ]
          },
          "minChainLength": 1,
          "chainLengthRange": -1,
          "eeType": [
            "app",
            "enrol"
          ]
        },
        {
          "subjectPermissions": {
            "explicit": [
              {
                "psid": 256,
                "sspRange": {
                  "all": null
                }
              }
            ]
          },
          "minChainLength": 1,
          "chainLengthRange": -1,
          "eeType": [
            "app",
            "enrol"
          ]
        }
```

```
      ],
      "verifyKeyIndicator": {
        "verificationKey": {
          "ecdsaNistP256": {
            "compressed-y-0": "length(256bit)"
                 or
            "compressed-y-1": "length(256bit)"
          }
        }
      }
    },
    "signature": {
      "ecdsaNistP256Signature": {
        "rSig": {
          "x-only": "length(256bit)"
        },
        "sSig": "length(256bit)"
      }
    }
  }
}
```

7.1.2 Intermediate CA Certificate Profile

```
{
  "version": 3,
  "type": "explicit",
  "issuer": {
    "sha256AndDigest": "49EA9FC96C6BA91A"
  },
  "toBeSigned": {
    "id": {
      "name": "ica.prod.s2x.io"
    },
```

```json
  "cracaId": "6BA91A",
  "crlSeries": 2,
  "validityPeriod": {
    "start": issuance timestamp,
    "duration": {
      "years": 25
    }
  },
  "appPermissions": [
    {
      "psid": 35,
      "ssp": {
        "opaque": "830002"
      }
    }
  ],
  "certIssuePermissions": [
    {
      "subjectPermissions": {
        "all": null
      },
      "minChainLength": 2,
      "chainLengthRange": 0,
      "eeType": [
        "app",
        "enrol"
      ]
    },
    {
      "subjectPermissions": {
        "explicit": [
          {
            "psid": 35,
            "sspRange": {
```

```
                              "all": null
                        }
                  },
                  {
                        "psid": 256,
                        "sspRange": {
                              "all": null
                        }
                  }
                ]
          },
          "minChainLength": 1,
          "chainLengthRange": -1,
          "eeType": [
                "app",
                "enrol"
          ]
        }
      ],
      "verifyKeyIndicator": {
        "verificationKey": {
          "ecdsaNistP256": {
                "compressed-y-0": "length(256bit)"
                      or
                "compressed-y-1": "length(256bit)"
          }
        }
      }
    },
    "signature": {
      "ecdsaNistP256Signature": {
        "rSig": {
          "x-only": "length(256bit)"
        },
```

```
      "sSig": "length(256bit)"
    }
  }
}
```

7.1.3 MA Certificate Profile

No MA certificate has been issued

7.1.4 Enrollment CA(ECA) Certificate Profile

Not applicable for this CPS.

7.1.5 Authorization CA(ACA) Certificate Profile

Not applicable for this CPS.

7.1.6 Enrollment Certificate Profile

Not applicable for this CPS.

7.1.7 RSU Certificate Profile

Not applicable for this CPS.

7.1.8 OBU Certificate Profile

Not applicable for this CPS.

7.2 CRL Profile

The format and content of the CRL issued by a CA or CRL Signer is aligned with IEEE 1609.2.1. The CRL is issued at least annually.

```
{
  "version": 1,
  "crlSeries": 256,
  "crlCraca": crl issuer id(8bytes),
  "issueDate": issuance timestamp,
  "nextCrl": next issuance timestamp,
  "priorityInfo": {
    "priority": 0
  },
  "typeSpecific": {
    "fullHashCrl": {
      "crlSerial": a counter that increments by 1 every time,
      "entries": SequenceOfHashBasedRevocationInfo
    }
  }
}
```

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

Compliance Audits are conducted at least annually.

8.2   Identity/Qualification of Assessor

Compliance audits of SAESOL Tech V2X Root CAs are performed by a public accounting firm that possesses the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit against the WebTrust Principles and Criteria for Certification Authorities;
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. Is a licensed WebTrust practitioner;
5. Is bound by law, government regulation, or a professional code of ethics; and
6. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3   Assessor's Relationship to Assessed Entity

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

8.4   Topics Covered by Assessment

Annual compliance audits of SAESOL Tech V2X Root CAs include an assessment of the controls SAESOL Tech V2X Root CA has implemented to ensure the secure operation of its CAs. In particular they cover an assessment of SAESOL Tech's compliance with the applicable WebTrust Principles and Criteria for Certification Authorities as published by CPA Canada.

The audit reports are published at https://www.saesol.tech/certificateauthority/.

8.5   Actions Taken as a Result of Deficiency

If a material deficiency in the design or operation of a control is identified during an audit, SAESOL Tech's CA Policy Authority determines whether remediating actions are required and how these will be implemented. SAESOL Tech seeks the input of its auditor regarding the remediation plans it makes and implements the remediation action within a commercially reasonable period of time.

8.6   Communication of Results

The Audit Report is made publicly available no later than three months after the end of the audit period. SAESOL Tech is not required to make publicly available any general audit findings that do not impact the overall audit opinion. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, SAESOL Tech provides an explanatory letter signed by its Auditor.

The Audit Report states explicitly which CAs, certification practices and locations it covers.

9 Other Business and Legal Matters

9.1   Fees

SAESOL Tech may charge Subscribers for the issuance and management of Certificates. SAESOL Tech does not charge for the revocation of certificates it has issued.

9.1.1 Certificate Issuance or Renewal Fees

SAESOL Tech does not charge a fee as a condition of making the CRLs required by this CPS available in a Repository or otherwise available to Relying Parties. SAESOL Tech may however charge a fee for providing customized CRLs, or other value-added revocation and status information services. SAESOL Tech does not permit access to revocation information, Certificate status information in its Repository by third parties that provide products or services that utilize such Certificate status information without SAESOL Tech's prior express written consent.

9.1.2 Certificate Access Fees

SAESOL Tech may charge a reasonable fee for access to its Certificate databases.

9.1.3 Revocation or Status Information Access Fees

SAESOL Tech may charge a reasonable fee for access to its Certificate databases.

9.1.4 Fees for Other Services

SAESOL Tech does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with SAESOL Tech.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following Applicant and Subscriber related information is considered confidential information.

- Certificate applications;
- Records submitted by the Applicant in support of Certificate applications;
- Private keys;
- Log files and other audit records;
- Transaction records.

9.3.2 Information Not Within the Scope of Confidential

Information

The following information shall not be considered confidential:

- Information included in Certificates,
- CA public Certificates,
- Information contained in this CPS document, and
- Any Certificate status or Certificate revocation reason code.

9.3.3 Responsibility to Protect Confidential Information

The CA observes applicable rules on the protection of personal data deemed by law or the SAESOL Tech's privacy policy (see section 9.4) to be confidential and is bound by the terms of its CPS and applicable legal agreements.

Subscribers are likewise bound by license agreement to confidentiality obligations.

9.4 Privacy of Personal Information

SAESOL Tech follows the Privacy Policy available at: 'Privacy Policy' at
`https://www.saesol.tech/certificateauthority/`. The personal data protection policy complies with the domestic laws of the Republic of Korea.

9.4.1 Privacy Plan

See Section 9.4.

9.4.2 Information Treated as Private

See Section 9.4.

9.4.3 Information not Deemed Private

Any information publicly available through a Certificate, CRL or their contents is not deemed private.

9.4.4 Responsibility to Protect Private Information

See Section 9.4.

9.4.5 Notice and Consent to Use Private Information

See Section 9.4.

9.4.6 Disclose Pursuant to Judicial or Administrative Process

See Section 9.4.

9.4.7 Other Information Disclosure Circumstances

See Section 9.4.

9.5   Intellectual Property Rights

SAESOL Tech protects its trademarks and respect those of others, seeking permission from owners before promoting any other company's trademark on its website or in conjunction with its service. Certificates issued by the CA are the exclusive property of SAESOL Tech. SAESOL Tech gives permission to reproduce and distribute certificates according to business agreement provided they are reproduced and distributed in full. SAESOL Tech reserves the right to revoke the certificate at any time and at its sole discretion. Subscriber private and public keys are the property of the Subscribers.

9.6   Representations and Warranties

9.6.1 CA Representations and Warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, SAESOL Tech does not make any representations regarding its products or services. To the extent permitted by applicable law SAESOL Tech disclaims any warranties, including any warranty of merchantability or fitness for a particular purpose.

9.6.2 RA Representations and Warranties

Not applicable.

9.6.3 Subscriber Representations and Warranties

Subscriber Commitments and Warranties

As part of the Subscriber Agreement or Terms of Use, SAESOL Tech requires Applicants to make the commitments and warranties outlined in this section for the benefit of both SAESOL Tech and the Certificate Beneficiaries.

Before issuing a Certificate, SAESOL Tech obtains, for its own benefit and that of the Certificate Beneficiaries, either:

- The Applicant's agreement to SAESOL Tech's Subscriber Agreement, or

- The Applicant's acceptance of SAESOL Tech's Terms of Use.

SAESOL Tech ensures that each Subscriber Agreement is legally binding on the Applicant or, in cases where SAESOL Tech itself is the Applicant, that the Terms of Use have been acknowledged. In either case, the agreement must explicitly apply to the Certificate being issued. SAESOL Tech may use electronic or

"click-through" agreements, provided they are deemed legally enforceable. A separate agreement may be executed for each Certificate request, or a single agreement may apply to multiple requests and resulting Certificates—so long as all Certificates issued are clearly covered by that agreement.

Obligations and Warranties in the Subscriber Agreement or Terms of Use

The Subscriber Agreement or Terms of Use includes provisions that impose the following obligations and warranties on the Applicant (or, if applicable, on behalf of the Applicant's principal, agent, subcontractor, or hosting provider):

1.
   Accuracy of Information

   + The Applicant must provide complete and accurate information in the certificate request and in any additional information requested by SAESOL Tech in connection with the Certificate issuance.
2.
   Protection of Private Key

   + The Applicant must take all reasonable measures to maintain exclusive control over, keep confidential, and protect the Private Key corresponding to the Public Key included in the requested Certificate(s), along with any related activation data or devices (e.g., passwords or hardware tokens).
3.
   Acceptance of Certificate

   + The Subscriber is responsible for reviewing and verifying the contents of the Certificate for correctness before using it.
4.
   Use of Certificate

   + The Certificate must be used exclusively for V2X purposes.

9.6.4 Relying Party Representations and Warranties

Relying Party Representations and Warranties

Relying Parties represent and warrant that:

(a) they have read, understood, and agreed to the terms set forth in this CPS;

(b) they have verified both the applicable SAESOL Tech Root V2X CA Certificate and all other certificates in the chain using the appropriate Certificate Revocation List (CRL) ;

(c) they do not use any Certificate that has been revoked or has expired;

(d) they possess sufficient information to make an informed decision regarding the degree to which they rely on the information contained in the Certificate;

(e) they have reviewed all applicable usage limitations and agree to the limitations of liability as set forth by SAESOL Tech regarding Certificate use;

(f) they are solely responsible for determining whether to rely on any Certificate information; and

(g) they bear full responsibility for any legal or other consequences resulting from their failure to meet the Relying Party obligations described in this CPS.

Relying Party Duty to Minimize Risk

Relying Parties further represent and warrant that they take all reasonable precautions to reduce risks associated with relying on digital signatures. This includes only relying on a Certificate after carefully considering the following factors:

- Applicable laws, including requirements for identity verification, data confidentiality or privacy, and the legal enforceability of the transaction;

- The intended use of the Certificate as described in either the Certificate itself or this CPS;

- The accuracy and relevance of the data included in the Certificate;

- The financial or transactional value of the communication or exchange;

- The potential harm or loss that could result from misidentification or a breach of confidentiality or privacy;

- The Relying Party's past interactions and experience with the Certificate Subscriber;

- Their general understanding of commercial practices and experience with electronic or digital transactions; and

- Any other indicators of trustworthiness or risk related to the Subscriber or the context of the communication, application, or transaction.

9.6.5 Representations and Warranties of Other Participants

Not applicable

9.7 Disclaimers of Warranties

Except as expressly stated in Section 9.6.1 of this CPS, all certificates and any related software and services are provided "as is" and "as available." To the maximum extent permitted by law, Saesol Tech disclaims all other warranties, both express and implied, including, without limitation, any implied warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided with respect to certificates issued by Saesol Tech, the CRL, and any participant's or third party's participation in the Saesol Tech PKI, including use of key pairs, certificates, the CRL, or any other goods or services provided by Saesol Tech to the participant.

Except as expressly stated in Section 9.6.1 of this CPS, SAESOL Tech does not warrant that any service or product meets any expectations or that access to certificates will be timely or error-free.

SAESOL Tech does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time. A fiduciary duty is not created simply because an individual or entity uses Saesol Tech's services.

9.8   Limitations of Liability

To the extent permitted by applicable law, SAESOL Tech shall not be liable for any direct, indirect, special, incidental, consequential, exemplary, or punitive damages, including but not limited to damages for lost data, lost profits, lost revenue, or the cost of procurement of substitute goods or services, however caused and under any theory of liability—including but not limited to contract or tort (including product liability, strict liability, and negligence)—whether or not SAESOL Tech was, or should have been, aware of the possibility of such damages, and even if any limited remedy provided herein fails of its essential purpose.

SAESOL Tech's total liability under this CPS is limited to $500.

9.9   Indemnities

1. As far as the law allows, Relying Parties are responsible for compensating SAESOL Tech if they: (a) break legal regulations, (b) fail to meet the commitments described in this CPS, (c) rely on a Certificate without good reason, or (d) do not confirm whether a Certificate is still valid or has been revoked.

9.10 Term and Termination

9.10.1   Term

New versions of this CPS supersede all previous versions and become effective upon publication in the Repository.

9.10.2   Termination

This CPS and any amendments remain in effect until replaced by a newer version.

9.10.3   Effect of Termination and Survival

Upon termination of this CPS, Participants are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates.

9.11 Individual Notices and Communications with Participants

9.12 Amendments

9.12.1   Procedure for Amendment

Section 1.5.4 describes the procedures and approval process for amending the CPS.

9.12.2   Notification Mechanism and Period

Section 1.5.4 describes the procedures and approval process for amending a CPS.

9.12.3   Circumstances Under Which OID Must be Changed

Not applicable.

9.13 Dispute Resolution Provisions

In the absence of specific contractual provisions, any dispute shall be resolved based on applicable laws and SAESOL Tech's internal procedures.

9.14 Governing Law

Laws governing SAESOL Tech V2X Root CA services are determined by applicable national and international legal and regulatory requirements.

9.15 Compliance with Applicable Law

SAESOL Tech V2X Root CA certification practices endeavors to comply with applicable national, provincial, local, and foreign laws, rules, regulations, ordinances, decrees, and orders, including but not limited to restrictions on exporting software, hardware, or technical information. This compliance is based on internal policy and applicable legal obligations.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 Severability

Not applicable

9.16.4   Enforcement (Attorney's Fees and Waiver of Rights)

Not applicable

9.16.5   Force Majeure

Not applicable

9.17 Other Provisions

Not applicable