INTEGRITY Security Services LLC Root Certificate Authority (CA)

Certificate Policy

Version 1.4
March 27, 2023

INTEGRITY Security Services LLC

TABLE OF CONTENTS

TABLE OF CONTENTS....2
1 INTRODUCTION....5
2 POLICY INFORMATION....7
2.1 Document Name and Identification....7
2.2 Purpose of this Certificate Policy (CP)....7
2.3 Relationship Between the CP and the CPS....7
2.4 CP Scope....7
2.5 Policy Administration....7
2.5.1 Organization Administering the Document....7
2.5.2 Person Determining CP and CPS Suitability for the Policy....8
2.5.3 CP Amendment and Approval Procedures....8
2.6 PKI Participants....8
2.6.1 Certification Authority....8
2.6.2 Relying Party....8
2.6.3 Subscriber....8
2.6.4 Applicant....8
2.6.5 Provider....9
2.7 Certificate Usage....9
2.7.1 Appropriate Certificate Uses....9
2.7.2 Prohibited Certificate Uses....9
3 DEFINITIONS AND ACRONYMS....10
3.1 Definitions....10
3.2 Acronyms....11
4 PUBLICATION AND REPOSITORY RESPONSIBILITIES....12
4.1 Publication of CA Information....12
4.2 Frequency of Publication....12
4.3 Access Controls on Repositories....12
5 IDENTIFICATION AND AUTHENTICATION....13
5.1 Naming....13
5.1.1 Hostname Specification....13
5.1.2 Uniqueness of Hostnames....13
5.1.3 Elector Group ID....13
5.1.4 Recognition, Authentication and Role of Trademarks....13
5.2 Initial Identity Validation....13
5.2.1 Method to Prove Possession of Private Key....14
5.2.2 Identity Authentication....14
5.2.2.1 Organization Identity Authentication....14
5.2.2.2 Individual Identity Authentication....14
5.3 Identification and Authentication for Revocation Request....14
5.4 Identification and Authentication for TBSCTL Signing....15

6 CERTIFICATE AND CTL LIFECYCLE OPERATIONAL REQUIREMENTS…16
6.1 Certificate Application and TBSCTL Signing Request.................................16
6.1.1 Certificate Application and TBSCTL Signing Request Qualifications.........16
6.1.2 Enrollment Process and Responsibilities...16
6.2 Certificate Application and TBSCTL Signing Request Processing..............16
6.2.1 Performing Identification and Authentication Functions............................17
6.2.2 Approval or Rejection of Certificate Applications......................................17
6.2.3 Approval or Rejection of TBSCTL Signing Requests................................17
6.2.4 Time to Process Certificate Applications and TBSCTL Signing Requests. 17
6.3 Certificate Issuance...18
6.3.1 CA Actions During Certificate or CTL Issuance..18
6.3.2 Notification to Subscriber by the CA of Certificate or CTL Issuance..........18
6.4 Certificate Acceptance...18
6.4.1 Conduct Constituting Certificate and CTL Acceptance.............................18
6.4.2 Publication of the Certificate and CTL by the CA......................................19
6.5 Key Pair and Certificate Usage...19
6.5.1 Subscriber Private Key and Certificate Usage..19
6.5.2 Relying Party Public Key and Certificate Usage.......................................19
6.6 Certificate Renewal..19
6.7 Certificate Rekey..20
6.8 Certificate and TBSCTL Modification..20
6.9 Certificate Revocation and Suspension...21
6.9.1 Circumstances for Certificate Revocation...21
6.9.2 Who Can Request Revocation?...22
6.9.3 Procedure for Revocation Request..22
6.10 CRL Issuance Frequency..23
6.11 CTL Issuance Frequency...23
6.12 Maximum Latency for CRLs..23
6.13 Maximum Latency for CTLs...23
6.14 OCSP Support..23
6.15 Key Escrow and Recovery...23
7 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS.....................24
7.1 IRCA Security Controls..24
7.2 Audit Logging Procedures...24
7.3 Records Archival..24
7.4 Key Changeover...25
7.5 IRCA Private Key Compromise and Disaster Recovery...............................25
7.5.1 Incident and Compromise Handling Procedures.......................................25
7.5.2 Business Continuity and Disaster Recovery...26
7.6 CA Termination...26
8 TECHNICAL SECURITY CONTROLS...27
8.1 Key Pair Generation...27

8.2 Private Key Protection....27
8.3 Public Key Delivery to ISS....27
8.4 TBSCTL Delivery to ISS....28
8.5 Root Certificate Operational Period and Key Pair Usage Period....28
8.6 Security Controls....28
9 CERTIFICATE AND CRL PROFILES....29
9.1 V2XRCA Profiles....29
9.1.1 V2XRCA Root Certificate Profile....29
9.1.2 V2XRCA CRL Profile....31
9.2 AUC2XRCA Profile....33
9.2.1 AUC2XRCA Root Certificate Profile....33
9.2.2 AUC2XRCA CRL Profile....34
9.2.2.1 CRL....34
9.2.2.2 Inner CRL....35
9.2.3 AUC2XRCA CTL Profile....36
9.2.3.1 CTL....36
9.2.3.2 Inner CTL....38
9.3 V2X Elector Profiles....41
9.3.1 V2X Elector Certificate Profile....41
9.3.1.1 ToBeSigned....41
9.3.1.2 Certificate....41
9.3.2 V2X CTL Profile....42
10 COMPLIANCE AUDIT AND OTHER ASSESSMENTS....43
10.1 Frequency of Assessment....43
10.2 Auditor's Relationship to Assessed Entity....43
10.3 Topics Covered by Assessment....43
10.4 Actions Taken as a Result of Deficiency....43
10.5 Communication of Results....43
10.6 Self-Audits....43
11 MISCELLANEOUS....44
11.1 Representations and Warranties....44
11.1.1 CA Representations and Warranties....44
11.1.2 Subscriber Representations and Warranties....44
11.2 Trademarks....45
11.3 Waivers....45
12 CONTACT....46
13 VERSION HISTORY....47

1 INTRODUCTION

BEFORE PROCEEDING, DOWNLOAD THE LATEST VERSION OF THIS DOCUMENT. THE DOWNLOAD LINK FOR THE LATEST VERSION OF THIS DOCUMENT IS IN THE CONTACT SECTION OF THIS DOCUMENT.

The INTEGRITY Security Services, Inc. ("ISS") Root CA Certificate Policy ("CP") describes the technical, business, and legal requirements governing the issuance and use of Root and Elector CA certificates ("Certificates") including, but not limited to, those from the ISS V2X Root CA ("V2XRCA"), the ISS V2X Electors, ISS V2G Root CAs (“V2GRCA”), and the ISS Australia C-ITS C2X Root CA ("AUC2XRCA") (collectively "IRCA"), by all users of those CAs including participants in SCMS Manager-approved vehicle-to-vehicle ("V2V"),vehicle-to-infrastructure ("V2I") and vehicle-to-grid (“V2G”) programs (collectively, "V2X"), including the US-DOT’s Connected Vehicle Pilot ("CV Pilot") program, and the car-to-car ("C2C"), car-to-infrastructure ("C2I") programs (collectively "C2X") as part of an ETSI-compliant C-ITS program, as well as other related services that leverage these certificate structures and associated public key infrastructures.

ISS established and operates these IRCAs to provide the generation, issuance, distribution, revocation, administration and management of the respective Root Certificate Authority’s or Elector’s ("CA") cryptographic key pair which is used to issue self signed certificates as well as to sign Certificates for authorized sub-CAs such as V2X Intermediate CAs ("ICAs"), the Policy Generator, the Misbehavior Detection Authority, and Certificate Revocation List ("CRL") generators, Enrolment Authorities and Authorization Authorities. The format of these V2XRCA and AUC2XRCA Certificates and their associated signatures shall be in accordance with IEEE 1609.2, ISO-15118 (2/20) or ETSI TS 103 097 as profiled by SCMS Manager or the ISS CA Advisory Board (ICAB).

ISS established and operates the Electors to provide the generation, issuance, distribution, revocation, administration and management of the respective Elector’s cryptographic key pair which is used to sign its Certificate as well as to sign Certificate Trust Lists (CTL) as directed by SCMS Manager. The format of these Elector Certificates, their signed CTLs and their associated respective signatures shall be in accordance with IEEE 1609.2 or X.509 as profiled by SCMS Manager.

This CP is part of the documents that govern the IRCA. Other documents include the Certification Practice Statements, Subscriber Agreements, and IRCA technical documentation.

Throughout this document key words are used to identify requirements. The key words "MUST", "MUST NOT", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", and "MAY" are used. These words are a subset of the IETF Request For Comments (RFC) 2119 key words, and have been chosen based on convention in other normative documents [RFC2119].

2 POLICY INFORMATION

2.1 Document Name and Identification

This document is the ISS Root CA Certificate Policy. You must obtain the latest version of this document by internet download or by contacting ISS using the information listed in the "Contact" section of this policy. The latest version of this document is immediately effective upon publication and it is your obligation to ensure you have such version. Revision history to this document is located in the "Version History" section of this document.

2.2 Purpose of this Certificate Policy (CP)

This Certificate Policy governs the IRCAs, the Certificates and Certificate Trust Lists (CTLs) they issue, and the purposes for which the issued Certificates and CTLs may be used.

2.3 Relationship Between the CP and the CPS

This CP states what assurance can be placed in a certificate or certificate trust list issued by the IRCA. The Certification Practice Statement (CPS) states how the IRCA establish that assurance. The IRCA issuing certificates and CTLs under this CP shall have a corresponding CPS.

2.4 CP Scope

This CP refers to the IRCA and the management team that generates, issues, distributes, revokes and manages cryptographic keys, Certificates and CTLs for IRCA Subscribers (as defined in the "Subscriber" section) who agree to be bound by the conditions set forth in this CP, the CPS, and the related Subscriber Agreement ("SA") and Relying Parties (as defined in "Relying Parties" section).

2.5 Policy Administration

2.5.1 Organization Administering the Document

This CP refers to the IRCA and the management team that generates, issues, distributes, revokes and manages cryptographic keys, Certificates and Certificate Trust Lists for both Subscribers (as defined in the "Subscribers" section) who agree to be bound by the conditions set forth in this CP and the respective Subscriber Agreements ("SA"), and Relying Parties (as defined in the "Relying Party" section).

The IRCAs are managed by the ISS Policy Authority ("IPA") which is composed of senior members of ISS appointed by ISS senior management. The IPA is responsible for this CP, the approval of related practice statements, and overseeing the conformance of CA practices with this CP. The IPA may be contacted with the information listed in the "Contact" section of this policy.

2.5.2 Person Determining CP and CPS Suitability for the Policy

The IPA shall determine the suitability and applicability of this CP and the conformance of the CPS to this CP for the IRCAs that issue Certificates and Certificate Trust Lists under this CP based on the results and recommendations received from an independent auditor (see the "Technical Security Controls" section).

The IRCAs must meet all requirements of the approved CPS before commencing operations. The IPA will make this determination based on the results and recommendations received from an independent auditor.

2.5.3 CP Amendment and Approval Procedures

The IPA is the only body with authority to approve this CP and any amendments to it. Amendments may be made by the IPA either by updating and publishing the entire document or by publishing a separate addendum. Subscribers and SCMS Manager (if for a US V2X system) will be notified by email and will have a fifteen (15) day review period to provide any feedback on the amendments before the IPA publishes the amended CP. The amendments are effective upon publication.

2.6 PKI Participants

2.6.1 Certification Authority

ISS' policies and practices are designed to ensure that the IRCAs comply in all material respects with the American Institute of Certified Public Accountants WebTrust Program for Certification Authorities.

The IRCAs shall materially comply with the respective Root CA and Elector requirements published from time-to-time by SCMS Manager and/or ICAB as determined by the IPA.

2.6.2 Relying Party

A "Relying Party" is an entity that relies on the validity of a Certificate or Certificate Trust List issued by any of the CAs governed by this CP.

2.6.3 Subscriber

A "Subscriber" is an organization that establishes a relationship with ISS as the operator of the IRCA through the respective Root CA Subscriber Agreements for the purpose of obtaining a Certificate containing the Public Key (as defined in the "Definitions" section) corresponding to the Subscriber's Private Key (as defined in the "Definitions" section). This Subscriber Agreement establishes the right and responsibilities of the parties regarding the issuance and management of Certificates.

2.6.4 Applicant

"Applicant" is in entity applying for Certificate service from the IRCA and who wishes to execute a Subscriber Agreement. An employee of Applicant who is authorized by the Applicant to act on the Applicant's behalf shall apply for the Certificate and agree to and accept the respective ISS Subscriber Agreement on the Applicant's behalf.

2.6.5 Provider

ISS is a “Provider” of Elector CA operations to SCMS Manager.

2.7 Certificate Usage

2.7.1 Appropriate Certificate Uses

The IRCAs shall be permitted to issue, manage, and revoke Certificates that enable the creation, operation or discontinuation of V2X sub-CAs ("Sub-CAs") and other entities including, but not limited to, the Policy Generator, Misbehavior Authority, Intermediate CAs, and CRL generators, Enrolment Authority and Authorization Authority. The IRCAs also shall be permitted to sign CRLs.

Each Sub-CA may create, manage, and destroy cryptographic keys and issue, manage, and revoke its Certificates and perform other functions as described in its applicable certification practice statement.

Further, pursuant to the explicit written direction of SCMS Manager, Elector CAs shall be permitted to issue, manage, and revoke their own Certificates as well as to sign CTLs provided to them by the SCMS Manager. Elector Certificates and CTLs signed by an Elector may only be issued to SCMS Manager and to no one else; SCMS Manager is responsible for their publication and dissemination.

2.7.2 Prohibited Certificate Uses

Certificates issued by the IRCAs shall not be used for any purpose other than those permitted in the "Appropriate Certificate Uses" section. Certificates and CTLs not explicitly authorized by SCMS Manager may not be processed or issued by the Electors and any such properly issued Certificates and signed CTLs shall not be used for any purpose other than those permitted in the "Appropriate Certificate and CTL Uses" section. In addition, Certificates and CTLs issued under this CP may not be used where prohibited by law.

3 DEFINITIONS AND ACRONYMS

3.1 Definitions

Applicant A legal entity applying for Certificate service from an IRCA and who wishes to execute a Subscriber Agreement.

Certificate A digitally signed bit string issued by an ISS RCA to a Subscriber identifying the holder ("Holder") of the Private Key corresponding to the Public Key contained in the Certificate.

Cryptoperiod The time period (or lifetime) during which a key may be used. Note for public key systems such as this Root CA, the private key Cryptoperiod will be different than the Cryptoperiod of the associated public key.

Elector An independent third party authorized by SCMS Manager to participate in a specific group of Electors whose function is to revoke a root CA or another Elector or add a root CA or another Elector to the V2X infrastructure.

GlobalCTL The CTL distributed by SCMS Manager with at least 3 Elector’s signatures appended

Key Pair For asymmetric key cryptography, a Private Key and its corresponding Public Key.

Private Key A secret key known only to Holder of the Key Pair. This is the key of a Key Pair that is used by the Holder to create digital signatures.

Public Key This key is mathematically related to the Holder’s Private Key. It may be publicly disclosed by the Holder and is used by Relying Parties to verify digital signatures created by the Holder using her Private Key.

Relying Party An entity that relies on the validity of a Certificate issued by an IRCA

Root CA A certificate authority that is at the highest level of a given PKI

Subordinate CA A certificate authority that lives between a Root CA and the end-entity certificates for a given PKI

Subscriber A legal entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement.

3.2 Acronyms

AU	Australia
AUC2XRCA	(ISS) Australia C2X Root CA
C-ITS	Cooperative Intelligent Transport Systems
C2C	C-ITS Car to Car
C2I	C-ITS Car to Infrastructure
C2X	C-ITS Car to All
CA	Certificate Authority or Certification Authority
CMS	(ISS) Certificate Management Service
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CTL	Certificate Trust List
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
ICA	Intermediate CA
ICAB	ISS CA Advisory Board
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPA	ISS Policy Authority
IRCA	(Collective reference to the) ISS Root and Elector Certificate Authorities
ISS	INTEGRITY Security Services LLC
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
RA	Registration Authority
SCMS	Security Credential Management System
TBS	To Be Signed
TBSCTL	To Be Signed CTL
TLM	Trust List Manager
TMR	(Australia Department of) Transport and Main Roads
US-DOT	United States Department of Transportation
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure
V2G	Vehicle to Grid
V2X	Vehicle to All
V2XRCA	(ISS) V2X Root Certification Authority

4 PUBLICATION AND REPOSITORY RESPONSIBILITIES

4.1 Publication of CA Information

Self-signed IRCA Certificates and associated CRLs shall be available in a publicly accessible repository.

Elector-signed CTLs may not be published; only SCMS Manager may publish a GlobalCTL.

The IRCA download information is in the "Contact" section of this document.

4.2 Frequency of Publication

Any new or modified CP or related CA information shall be published within seven (7) business days of its approval. In the event that the IPA determines that changes to the CP are necessary or desirable, ISS will provide a fifteen (15) day review period (Review Period) to all then current Subscribers to which Certificates have been issued and which have not expired or been revoked. This review period may include SCMS Manager if such changes affect an Elector. Such updates become binding upon being published for all Subscribers and for all Certificates and for all Certificate Trust Lists issued or to be issued.

4.3 Access Controls on Repositories

The IRCAs shall protect information not intended for public dissemination or modification. IRCA Certificates and CRLs in the repositories shall be publicly available through the Internet. The CPS shall detail what information in the repositories shall be exempt from automatic availability and to whom, and under which conditions the restricted information may be made available.

5 IDENTIFICATION AND AUTHENTICATION

5.1 Naming

5.1.1 Hostname Specification

The ISS V2X Root CA, the ISS V2X Electors and the ISS C-ITS C2X Root CA Certificates are based on IEEE 1609.2. Hostnames (also known as subject names in X.509 parlance) are UTF8String (SIZE (0…255)) and may be selected by the Subscriber so long as part of the selected hostname identifies the host's function. The acceptable host function identifiers are: **elector** for an Elector CA, **rootca** for the Root CA, **ica** for Intermediate CA, **ma** for Misbehavior Authority, **pg** for Policy Generator, **crlg** for CRL Generator, **aa** for Authorization Authority, and **ea** for Enrollment Authority. The hostnames must be meaningful. ISS, at its sole discretion, may refuse to issue a Certificate with a hostname not meeting these requirements.

The V2X Root CAs following the X.509 structure should use conventional subject names. Subject names must be meaningful. ISS, at its sole discretion, may refuse to issue a Certificate with a subject name not meeting these requirements.

5.1.2 Uniqueness of Hostnames

The V2XRCA, AUC2XRCA and management team will ensure that all hostnames are unique in the Certificates issued by these IRCAs.

For Electors, the IRCA management team will confirm that the hostnames are unique with SCMS Manager.

For V2RGCAs, the IRCA management team will confirm that the hostnames are unique with SCMS Manager.

5.1.3 Elector Group ID

For the TBSCTL and CTL, the electorGroupId value shall be zero.

5.1.4 Recognition, Authentication and Role of Trademarks

Subscribers may not request Certificates with any content that infringes the intellectual property rights of another entity. This CP does not require that an Applicant's right to use a trademark be verified; however, ISS may reject any application or require revocation of any Certificate that is part of a trademark or intellectual property dispute or if ISS has reason to believe that such application or Certificate infringes a third party's intellectual property.

5.2 Initial Identity Validation

For a prospective root CA subscriber, ISS shall use any legal means of communication or investigation to ascertain the identity of an Applicant. ISS may refuse to issue a Certificate at its sole discretion.

Since an Elector only responds to requests from SCMS Manager, ISS does not need to validate the organization, but does need to validate the identities of the individuals claiming to act on its behalf. This validation process may lead ISS to refuse to issue a CTL.

5.2.1 Method to Prove Possession of Private Key

For Certificate Signing Requests ("CSRs"), Subscribers must submit a properly formed certificate body that is self-signed to establish both authenticity and integrity of the request. Additional CSR requirements are outlined in the Subscriber Agreement "Certification Signing Request" section.

Note that an Elector CA does not issue certificates other than its own self-signed certificate.

5.2.2 Identity Authentication

5.2.2.1 Organization Identity Authentication

Applicants shall submit their name, address and documentation of their status as a legal entity as part of the application process. The legal status of all Applicants shall be verified using reliable third party and government databases or through other direct means of communication with the entity or jurisdiction governing the entity's legal creation, status, or recognition. If such efforts are insufficient to confirm the legal existence and identity of the entity, the Applicant may be required to provide legal documentation.

The IPA shall verify the information submitted by the Applicant in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the Applicant.

5.2.2.2 Individual Identity Authentication

Subscribers must provide the names of two individuals who are authorized ("Authorized Individuals") to act on the Applicant's/Subscriber's behalf for correspondence with ISS. Authorized Individuals acting on behalf of Applicants and Subscribers shall be authenticated by ISS as part of the Subscriber Agreement process.

SCMS Manager must provide the names of four individuals who are authorized ("Authorized Individuals") to act on the its behalf for correspondence with ISS regarding Elector operation. Authorized Individuals acting on behalf of SCMS Manager shall be authenticated by ISS prior to the issuance of Elector certificates.

5.3 Identification and Authentication for Revocation Request

All revocation requests shall be authenticated by ISS.

A Subscriber shall request the revocation of its Certificate in email, carbon copied to all Authorized Individuals and appropriate Subscriber senior executive, with a paper letter requesting the same, signed by both Authorized Individuals or an Authorized Individual and a senior executive of the Subscriber, and sent by overnight courier to the ISS RCA Administrator.

The IRCA contact information is listed in the "Contact" section of this document.

ISS shall confirm the written request details with at least one of the Authorized Individuals and the senior executive prior to acting on the revocation request.

5.4 Identification and Authentication for TBSCTL Signing

ISS requires SCMS Manager to request the signing of a TBSCTL in email, carbon copied to all Authorized Individuals and the SCMS Manager president, with a paper letter requesting the same, signed by two Authorized Individuals and the SCMS Manager president, and sent by courier with tracking information to the IPA.

The IPA contact information is listed in the "Contact" section of this document.

ISS shall confirm the written request details by telephone and email with at least two of the Authorized Individuals who are different from the request signatories prior to acting on the TBSCTL Signing request.

6 CERTIFICATE AND CTL LIFECYCLE OPERATIONAL REQUIREMENTS

This section describes the policies related to the management of the Certificate and CTL lifecycle by ISS.

6.1 Certificate Application and TBSCTL Signing Request

The Certificate application process must provide sufficient information to:

- Establish the applicant's or SCMS Manager's authorization to obtain a Certificate or CTL per the "Identity Authentication" section.
- Establish and record Applicant or SCMS Manager's identity per the "Identity Authentication" section.
- For a Certificate request, obtain the Subscriber's public key and verify the Subscriber's possession of the private key for each Certificate required per the "Method to Prove Possession of Private Key" section.
- For a TBSCTL signing request, confirm the request per the "Identification and Authentication for TBSCTL Signing" section.
- Verify any role or authorization information requested for inclusion in the Certificate.
- Verify the information requested for inclusion in the CTL per the "Identification and Authentication for TBSCTL Signing" section

These steps may be performed in any order that is convenient for the IRCA Administrator and Applicants/Subscribers/SCMS Manager that does not defeat security, but all must be completed before Certificate or CTL issuance.

6.1.1 Certificate Application and TBSCTL Signing Request Qualifications

Only Subscribers' Authorized Individuals may submit a Certificate application. Only SCMS Manager's Authorized Individuals may submit a TBSCTL signing request. No individual listed on a government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the United States may submit an application for a Certificate.

6.1.2 Enrollment Process and Responsibilities

ISS is responsible for verifying the identity of individuals and entities in accordance with this CP prior to authorizing issuance of a Certificate or a CTL. Each Applicant and SCMS Manager individual shall submit sufficient information and documentation for ISS to perform the required verification of identity prior to issuing a Certificate or CTL.

All communications during the Certificate application process or TBSCTL signing process shall be authenticated and protected from modification.

6.2 Certificate Application and TBSCTL Signing Request Processing

ISS shall verify the accuracy of information in Certificate applications before Certificates are issued.

ISS shall verify the accuracy of information in a TBSCTL signing request before a CTL is issued.

6.2.1 Performing Identification and Authentication Functions

ISS shall identify and verify each Applicant and SCMS Manager individually in accordance with the "Initial Identity Validation" section. Additional requirements are listed in the Subscriber Agreement and CPS.

6.2.2 Approval or Rejection of Certificate Applications

Any Certificate application that is received by ISS under this policy, for which the identity and authorization of the Authorized Individual has been validated and authenticated, will be duly processed. However, ISS shall reject any application for which such validation and authentication cannot be completed, or when ISS has cause to lack confidence in the application or certification process, or if the IEEE 1609.2/ETSI TS 103 097 (or their then current successors), or X.509 Certificate fields as profiled by SCMS Manager, ICAB, or IPA are inappropriately configured in the CSR.

ISS will notify the Subscriber upon approval or rejection of its Certificate application within three (3) business days.

6.2.3 Approval or Rejection of TBSCTL Signing Requests

Any TBSCTL signing request that is received by ISS under this policy, for which the identity and authorization of the Authorized Individuals have been validated and authenticated, will be duly processed. However, ISS shall reject any signing requests for which such validation and authentication cannot be completed, or when ISS has cause to lack confidence in the request, or if the IEEE 1609.2 (or its then current successor) TBSCTL fields as profiled by SCMS Manager are inappropriately configured in the request.

ISS will notify SCMS Manager upon approval or rejection of its TBSCTL signing request within a minimum of 24 hours if the request is for removal of either a root CA or another Elector; otherwise, it will be processed within 3 business days.

6.2.4 Time to Process Certificate Applications and TBSCTL Signing Requests

Certificate applications will be processed, and a Certificate will be issued within sixty (60) calendar days of successful verification.

CTLs for removal of a root CA or another Elector will be produced from a successfully verified TBSCTL signing request within 48 hours of the TBSCTL signing request’s receipt by ISS.

CTLs to add a root CA or another Elector will be produced from a successfully verified TBSCTL signing request within a minimum of 5 business days of the TBSCTL signing request’s receipt by ISS

6.3 Certificate Issuance

6.3.1 CA Actions During Certificate or CTL Issuance

Upon receiving the request, the IRCA will:

- Verify the identity of the requester;
- Verify the authority of the requester and the integrity of the information in the certificate request or the TBSCTL signing request;
- Build and sign a requestor’s TBS if all certificate or CTL requirements have been met;
- Make the Certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged their obligations as described in the "Subscriber Representations and Warranties" section.
- Make the CTL available to SCMS Manager.

This Certificate or CTL will not be created until all verifications and modifications, if any, have been completed to the IRCA’s satisfaction.

All TBS field information received from a Subscriber or SCMS Manager shall be verified before inclusion in a Certificate or CTL. The responsibility for verifying prospective subscriber/SCMS Manager data shall be described in the CPS.

ISS shall verify that the identified and authenticated Subscriber is the source of the Certificate request and that the Subscriber is the entity that will be issued the Certificate. Databases used to confirm Subscriber identity information shall be protected from unauthorized modification or use. ISS actions during the Certificate issuance process shall be performed in a secure manner.

6.3.2 Notification to Subscriber by the CA of Certificate or CTL Issuance

ISS shall notify the Subscriber within the fifteen (15) day certificate application processing window of Certificate issuance and may use any reliable mechanism to deliver the Certificate to the Subscriber.

ISS shall notify the SCMS Manager within two hours of CTL issuance and may use any reliable mechanism to deliver the CTL to SCMS Manager.

6.4 Certificate Acceptance

6.4.1 Conduct Constituting Certificate and CTL Acceptance

ISS shall confirm with the Subscriber that it has received and validated the Certificate. Failure by the Subscriber to acknowledge the correctness of the Certificate within three (3) business days of issuance may result in ISS revoking the Certificate.

ISS shall confirm with SCMS Manager that it has received and validated the Certificates and CTL(s) for the ISS Elector(s). If a Certificate or CTL is rejected by SCMS Manager, ISS and SCMS Manager will identify the reason for rejection and a new Certificate or CTL will be issued by ISS to SCMS Manager and confirmed that it is correct and accepted by SCMS Manager.

6.4.2 Publication of the Certificate and CTL by the CA

ISS shall make the IRCA root certificates ("Root Certificates") and any issued Certificate available by sending it to the Subscriber or SCMS Manager. Similarly, ISS shall make Elector signed CTLs available by sending them to SCMS Manager.

6.5 Key Pair and Certificate Usage

6.5.1 Subscriber Private Key and Certificate Usage

Root CA Subscribers must use the keys in their Certificates for their intended purposes, using the following policies and procedures:

V2XRCA:	IEEE 1609.2
AUC2XRCA:	ETSI TS 103 097 and TS 102 941
V2GRCA:	ISO15118 and X.509
All:	IPA-approved documentation

ISS shall use the keys in their Elector Certificates for their intended purposes, using the following standards, policies and procedures:

V2X Elector:	IEEE 1609.2 & SCMS Manager Elector Policy

All Subscribers and ISS must protect their respective Private Keys associated with their respective Public Keys in their Certificates from unauthorized use or disclosure and use reasonable means to prevent any such unauthorized use and disclosure, as specified in SCMS Manager, ICAB and the Subscriber Agreement documentation. Should there be a conflict in these referenced documents, the Subscriber Agreement shall prevail.

6.5.2 Relying Party Public Key and Certificate Usage

Relying Party software shall be compliant with IEEE 1609.2 and ETSI TS 102 941 and TS 103 097 as profiled per SCMS Manager, ICAB, or X.509 and ISO-15118, and/or IPA-approved documentation and standards. Verifying the validity of issued Certificates is solely the responsibility of the Relying Parties. ISS shall publish revoked issued Certificates in its repository as a CRL. The repository location is listed in the "Contact" section of this document.

ISS' V2XRCA or Elector certificate, if revoked by SCMS Manager, will not be contained in a CRL but will be identified by its absence from the next GlobalCTL published by SCMS Manager.

Relying Parties must check the applicable CRL and the SCMS Manager-published GlobalCTL as part of their verification and validation process.

6.6 Certificate Renewal

Certificate renewal is not supported by the IRCA system.

6.7 Certificate Rekey

Rekeying a Certificate consists of creating a new Certificate with a different subject Public Key while retaining the remaining contents of the old Certificate that describe the subject (e.g., hostname and permissions). The new Certificate may be assigned a different validity period, specify a different CRL, and/or be signed with a different key.

Subscribers seeking rekey of Certificates shall identify and authenticate themselves for the purpose of rekeying as described in the "Initial Identity Validation" section, and the rekey request must include a new CSR containing a new Public Key. Re-use of old previously certified private/public key pairs is not allowed.

ISS shall validate the re-key request information prior to issuing a new Certificate. This validation will include a check with at least one of the Authorized Individuals acting on the Subscriber’s behalf.

ISS shall issue a Certificate for a valid rekey request. ISS shall notify the Authorized Individuals of the Subscriber, and it may use any reliable mechanism to deliver the Certificate to the Subscriber. ISS shall contact the Subscriber to confirm receipt of the issued Certificate.

After re-keying a client Certificate, ISS will revoke the old Certificate unless requested by Subscriber to not revoke the old Certificate for a specific time period in order to accommodate the Subscriber’s shift to the new Certificate. In any event, ISS shall not further re-key, renew, or modify the old Certificate.

After re-keying an Elector Certificate, SCMS Manager will issue a new TBSCTL for the new Certificate and cause a GlobalCTL to be created and issued. In any event, ISS does not further re-key, renew, or modify the old Elector Certificate.

6.8 Certificate and TBSCTL Modification

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to permissions) provided that the modification otherwise complies with this CP. The new Certificate shall have the same subject Public Key. Additional examples of circumstances when Certificate modification may occur include minor name changes and the replacement of the Certificate where a minor error in Certificate information or profile has been discovered.

After modifying a Certificate, ISS shall revoke the old Certificate if it has been distributed by the Subscriber to Relying Parties. If the Subscriber has not used the old Certificate, both parties shall destroy it to prevent its dissemination. ISS shall not further re-key, renew, or modify the old Certificate.

ISS may modify Certificates at its own discretion or upon request of a Subscriber. Upon receiving a request for modification, ISS shall verify any information that will change in the modified Certificate. ISS may issue the modified Certificate only after completing the verification process, which may include telephonically contacting the Subscriber. The validity period of a modified Certificate shall not extend beyond the authorized duration (see the "Technical Security Controls" section)

For Elector Certificates and TBSCTLs, ISS will not modify their respective fields once approved by SCMS Manager.

6.9 Certificate Revocation and Suspension

This section describes Certificate revocation by the IRCA system. Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period.

The IRCA operating under this policy shall issue CRLs covering all revoked but unexpired Certificates issued under this policy.

The IRCA operating under this policy shall make public a description of how to obtain revocation information for the Certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to Subscribers during certificate request or issuance and shall be readily available to any potential relying party.

Certificate suspension is not supported by the IRCA system.

6.9.1 Circumstances for Certificate Revocation

Revocation may occur via:

- Direct revocation by ISS
- Indirectly via the Electors for V2XRCA or an ISS Elector
- Indirectly via the AU TLM for the AUC2XRCA

Reasons for the revocation are as follows:

- The Subscriber has requested revocation of its Certificate;
- ISS has requested revocation of its Elector
- SCMS Manager or the IRCA management team has reason to believe an Elector or CA Private Key has been compromised;
- The IRCA management team has reason to believe the Subscriber is violating the terms and conditions of this CP;
- SCMS Manager has reason to believe ISS is violating the terms and conditions of the CP;
- The binding between the subject and the subject’s Public Key in the Certificate is no longer valid;
- SCMS Manager or the IRCA management team receives and validates an authorized report of misbehavior from SCMS Manager or an ICAB or IPA authorized misbehavior authority or authorized representative of US-DOT or AU TMR;
- The Subscriber's or IRCA’s management team has reason to believe the Subscriber's Certificate was issued in a manner materially non-compliant with this CP, the CPS, or the applicable Subscriber Agreement;
- The Subscriber's or IRCA’s management team has reason to believe the Subscriber's practices are materially non-compliant with the Subscriber's CP or CPS and such non-compliant practices will not be remedied or mitigated within a reasonably short period, generally not to exceed thirty (30) calendar

days, and the IPA believes continued use of that Certificate is harmful to the IRCA ecosystem;

- SCMS Manager has reason to believe ISS' practices are materially non-compliant with the CP or CPS and such non-compliant practices will not be remedied or mitigated within a reasonably short period, generally not to exceed thirty (30) calendar days, and SCMS Manager believes continued use of that Elector Certificate is harmful to the SCMS Manager ecosystem;
- The Subscriber is violating the terms and conditions of the Subscriber Agreement;
- ISS received a lawful and binding order from a government or regulatory body to revoke the Certificate;
- The Subscriber was added as a denied party or prohibited person to a blacklist, or it is operating from a destination prohibited by US law; or
- The V2XRCA root certificate is revoked by the Electors or the AUC2XRCA is removed from the Certificate Trust List by the AU Trust List Manager.

Whenever a decision is reached to proceed with a revocation, the associated Certificate shall be revoked and placed on the CRL. Revoked Certificates shall be included on all new publications of the certificate status information until the Certificates expire.

For an Elector, SCMS Manager will revoke it by issuing a new GlobalCTL with that Elector removed from it.

6.9.2 Who Can Request Revocation?

ISS shall accept revocation requests from authenticated and authorized parties, such as the Subscriber, authorized US-DOT representative, or authorized TMR representative. ISS may establish procedures that allow other entities to request Certificate revocation for fraud or misuse. ISS may revoke a Certificate of its own volition to safeguard the trust in the IRCA ecosystem even if no other entity has requested revocation, after a three (3) day notice to Subscriber or SCMS Manager, unless a shorter time period is necessary due to criticality.

6.9.3 Procedure for Revocation Request

Entities submitting Certificate revocation requests must list their identity and explain the reason for requesting revocation. ISS shall authenticate and log each revocation request. ISS shall revoke a Certificate if the request is authenticated as originating from the Subscriber for its Certificate or for Certificates under its purview. If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, ISS shall investigate the alleged basis for the revocation request.

ISS shall maintain a 24/7 support contact mechanism to capture any reporting of a Certificate problem. ISS must respond within a reasonable period of time. If appropriate, ISS may forward complaints to law enforcement. The IRCA systems shall list revoked Certificates in its CRL where they will remain until the end of their validity period.

6.10 CRL Issuance Frequency

ISS shall issue IRCA CRLs at least every five (5) years, and not more than 30 calendar days after it has been determined that revocation of a Certificate is required.

ISS shall retain all entries in the IRCA CRL issued by it until the revoked Certificates expire. The system is not obliged to retain any expired or revoked Certificates.

6.11 CTL Issuance Frequency

ISS shall issue a new CTL only in response to a request received from SCMS Manager to add or remove a Root CA or Elector from the SCMS Manager-approved ecosystem.

6.12 Maximum Latency for CRLs

CRLs shall be published within five (5) business days of generation during normal operation. In the event of a disaster at the primary site, if required, CRLs will be published within one (1) business day from activation of the disaster recovery site.

Furthermore, each CRL shall be published no later than the time specified in the *nextUpdate* field of the previously issued CRL for same scope.

6.13 Maximum Latency for CTLs

A CTL issued to remove a Root CA or Elector shall be published within a minimum of 48 hours and a maximum of 3 business days after a request is received from SCMS Manager.

A CTL issued to add a Root CA or Elector shall be published within a minimum of five (5) business days and a maximum of one calendar quarter after a request is received from SCMS Manager.

In the event of a disaster at the primary site, if required, CTLs will be published within one (1) business day from activation of the disaster recovery site.

6.14 OCSP Support

V2GRCA certificates will also support validation using the Online Certificate Status Protocol (OCSP). Each V2GRCA certificate will include a network address where the corresponding OCSP service handler can be contacted.

6.15 Key Escrow and Recovery

IRCA private keys are never escrowed.

7 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

This section describes the non-technical security controls used by the IRCA system to perform the functions of key generation, subject authentication, Certificate issuance, Certificate revocation, CTL issuance, audit, and archival.

7.1 IRCA Security Controls

Critical IRCA operations take place within secure facilities to which access is limited to authorized personnel. Cryptographic hardware is physically segregated from the organization's other systems. Access to such systems is controlled by multiple layers of physical security controls, providing reasonable assurance that access is only granted to individuals who require such access to fulfill their job responsibilities.

Details of the IRCA security controls are documented in internal ISS documents. These policies are not publicly disclosed but are reviewed within the scope of WebTrust for Certification Authorities.

These policies document controls related to the following:

- Physical site construction
- Physical access controls,
- Environmental controls,
- Operational controls, and
- Personnel security controls.

7.2 Audit Logging Procedures

As an offline CA, event logging only occurs when an IRCA is activated. All operator actions are logged and reviewed following each activation by an internal auditor. The logs must be removed from the IRCA by an ISS administrator and as part of an approved activity. The ISS administrator is a different person from those who control the signing key. The auditor will report any unusual events to the IPA for analysis and resolution. All available logs may be subject to audit by the independent auditor.

7.3 Records Archival

ISS shall include enough detail in its archived records to show that a Certificate or CTL was issued in accordance with the CP. ISS shall retain the following information in its archives regarding its operation:

1. Any accreditation of the specific IRCA
2. CP and CPS versions
3. Contractual obligations and other agreements concerning the operation of the CA
4. System and equipment configurations, modifications, and updates
5. Certificate and revocation requests
6. Identity authentication data
7. Any documentation related to the receipt or acceptance of a Certificate or token
8. Subscriber Agreements

9. Issued Certificates
10. A record of Certificate re-keys
11. Other signed files such as CRLs and CTLs
12. Any data or applications necessary to verify an archive's contents
13. Compliance auditor reports
14. Any changes to the specific IRCA audit parameters
15. Event and audit logs, including identified attempts to delete or modify the logs
16. Key generation actions
17. Access to Private Keys for key recovery purposes
18. Changes to trusted Public Keys
19. *m of n* splitting of Private Keys
20. Approval or rejection of a Certificate status change request
21. Appointment of an individual to a trusted role
22. Destruction of a cryptographic module
23. Certificate compromise notifications
24. Remedial action taken as a result of violations of physical security
25. Violations of the CP or CPS

All records will be archived in a secure offsite location and retained for a period of five (5) years from their dates of origination. No unauthorized person may read, modify, or delete the archives.

7.4 Key Changeover

ISS will change IRCA Key Pairs periodically. After key change, ISS shall sign Certificates using only the new Private Key. ISS shall destroy its old IRCA Private Key and shall make the old IRCA Certificate available to verify signatures until all Certificates signed using the old Private Key have expired.

7.5 IRCA Private Key Compromise and Disaster Recovery

7.5.1 Incident and Compromise Handling Procedures

If ISS suspects that an IRCA Private Key is compromised or lost then ISS shall immediately assess the situation, determine the degree and scope of the incident, and notify its current Subscribers and either SCMS Manager or ICAB depending upon the affected Root CA or Elector CA. ISS personnel shall report the results of the investigation to the IPA, ISS Executive Management, its current Subscribers, and either SCMS Manager or ICAB depending upon the affected Root CA or Elector CA. The report must detail the cause of the compromise or loss and the measures which should be taken to prevent a reoccurrence.

If it is determined that an IRCA Private Key was compromised, the IPA will inform either the SCMS Manager or ICAB so the particular IRCA Certificate can be revoked by them.

7.5.2 Business Continuity and Disaster Recovery

An IRCA Private Key is split in an *m of n* procedure (with *m* equal or greater than 2) with a enough shares to restore the key distributed at least 100 miles away from the IRCA facility. For disaster recovery from the incapacitation/destruction of the primary CA site, ISS will instantiate a second IRCA at an alternate secure location and restore the Private Key from the *m of n* splits.

7.6 CA Termination

The V2XRCA system can only be terminated by the Electors voting to revoke the CA or by ISS Executive Management. The AUC2XRCA system can only be terminated by TMR agreeing to revoke the CA or by ISS Executive Management. In the event the CA is terminated, all Certificates issued by the CA will be revoked and the CA will cease to issue Certificates. If ISS terminates an IRCA system, the IPA will provide a minimum of 365 days' notice (Notice Period) to all then current Subscribers to which Certificates have been issued and which have not expired or been revoked. During this Notice Period, ISS will coordinate the transition of the terminating IRCA system to another CA entity established or agreed-upon by the Subscribers in order to continue service. For ISS to complete this transition, a simple majority of the then-current Subscribers must agree to the transition to the new entity. Should a simple majority not agree to the transition, then ISS will terminate the IRCA at the end of the Notice Period. Upon termination, the records of the CA will be archived and retained for a period of two (2) years.

Elector CAs may be terminated by SCMS Manager or by ISS Executive Management. Should ISS terminate an Elector, it will provide six months’ notice to SCMS Manager. During this Notice Period, ISS will coordinate the transition of the Elector to another entity approved by SCMS Manager. Should no other entity be approved by SCMS Manager, ISS will terminate the Elector at the end of the Notice Period. Upon termination, the records of the Elector CA will be archived and retained for a period of two (2) years.

8 TECHNICAL SECURITY CONTROLS

8.1 Key Pair Generation

All Key Pair generation must be achieved using a Hardware Security Module ("HSM"), which has been NIST validated as meeting Federal Information Processing Standards ("FIPS") 140-2 Level 3 or higher.

The key pairs generated must be NIST or Brainpool approved key types.

When generating keying material, the IRCA shall create auditable evidence to show that ISS enforced role separation and followed its key generation process. ISS shall have an independent third-party auditor validate the execution of the key process by either witnessing the key generation or by examining the signed and documented record of the key generation.

Subscribers must generate their elliptic curve cryptography ("ECC") key pairs for Certificate signing using an HSM that has been NIST validated as meeting FIPS 140-2 Level 3 at a minimum.

8.2 Private Key Protection

The HSM for generating and storing an IRCA Private Key shall be minimally certified to FIPS 140-2 Level 3 or higher. There shall be a separation of physical and logical access to the IRCA’s Private Key to this extent:

- A minimum of two individuals are required for physical access to the hardware.
- If an IRCA's Private Key requires disaster recovery, a secret splitting method consisting of individuals, passphrases, and *m* of *n* removable tokens is required for logical reconstruction. When an IRCA signing pair is changed, the old *m of n* key shares shall be physically destroyed.
- An IRCA Private Key shall never be exported from the HSM as plaintext.
- An IRCA Private Key shall never be escrowed or archived except for the *m* of *n* secret splitting method described above.

Subscribers’ private signing keys must be similarly generated and protected; however, the Subscribers may backup their private keys using alternate methods so long as they are kept securely in a corporate vault or safe deposit box, and that at least three (3) individuals are required to physically access the splits and restore the private keys.

8.3 Public Key Delivery to ISS

Subscribers shall use a self-signed certificate of the appropriate IEEE 1609.2 or ETSI TS103 097 structure for the entity the certificate is being requested to deliver their Public Key to ISS and the appropriate IRCA system. This message format provides proof-of-possession of the Private Key associated with the Public Key. ISS shall confirm that it has correctly received the Public Key from the Subscriber prior to issuing a Certificate for the Public Key.

8.4 TBSCTL Delivery to ISS

ISS only accepts TBSCTLs sent by SCMS Manager in the proper format and that can be validated with SCMS Manager. ISS authenticates and validates the integrity of all TBSCTL signing requests.

8.5 Root Certificate Operational Period and Key Pair Usage Period

The IRCAs shall follow the recommended Certificate operational periods and private key cryptoperiods as specified by the IPA or SCMS Manager. The V2XRCA Private Key shall have a Cryptoperiod of 20 years and its Root Certificate shall have a 70-year lifetime. At the end of its Cryptoperiod, the private key will be destroyed.

8.6 Security Controls

IRCA computer security controls shall be designed to meet or exceed the policies set by WebTrust for Certification Authorities, v2.0 or its then current version at the time of audit.

IRCA computer security controls include support for the following areas:

- Activation Data
- Computer and Network Security
- Lifecycle Technical Controls
- Time Stamping

9 CERTIFICATE AND CRL PROFILES

9.1 V2XRCA Profiles

The V2XRCA Certificate Profile and CRL Profile shall materially conform to IEEE 1609.2-2016 as profiled by the IPA and approved by SCMS Manager. The required profiles are specified in the following sections.

9.1.1 V2XRCA Root Certificate Profile

```
IEEE1609dot2-profiles {iso(1) identified-organization(3) ieee(111)
standards-association-numbered-series-standards(2) wave-stds(1609)
dot2(2) base (1) profiles (3)}

DEFINITIONS AUTOMATIC TAGS ::= BEGIN

EXPORTS ALL;

IMPORTS
  Certificate,
  Countersignature,
  ExplicitCertificate,
  ImplicitCertificate,
  PsidGroupPermissions,
  PsidSsp,
  SequenceOfPsidGroupPermissions,
  SequenceOfPsidSsp,
  SequenceOfPsidSspRange
FROM IEEE1609dot2 {iso(1) identified-organization(3) ieee(111)
    standards-association-numbered-series-standards(2) wave-stds(1609)
    dot2(2) base(1) schema(1)}

  CrlSeries,
  Psid,
  PsidSspRange,FROM IEEE1609dot2BaseTypes {iso(1) identified-organization(3) ieee(111)
standards-association-numbered-series-standards(2) wave-stds(1609)
dot2(2) base(1) base-types(2)}

  CrlPsid::= Psid (256)
FROM IEEE1609dot2Crl {iso(1) identified-organization(3) ieee(111)
  standards-association-numbered-series-standards(2) wave-stds(1609)
  dot2(2) crl(3) protocol(2)}

  CrlSsp,
  PermissibleCrls
FROM IEEE1609dot2CrlSsp {iso(1) identified-organization(3) ieee(111)
    standards-association-numbered-series-standards(2) wave-stds(1609)
    dot2(2) crl(3) service-specific-permissions (3)}

  RootCaCertExpiration,
  BsmPsid::= Psid(32), --0x20
  MisbehaviorReportingPsid::= Psid(38),  --0x26
  SecurityMgmtPsid::= Psid(35),  --0x23
  ScmsSpclComponentCrlSeries::= CrlSeries (256)
FROM Ieee1609dot2ScmsBaseTypes {iso(1) identified-organization(3) ieee(111)
standards-association-numbered-series-standards(2) wave-stds(1609)  dot2(2)
scms (2) interfaces(1) base-types (2)}
;
----------------------------------------------
--                  Root Certificate Authority
----------------------------------------------
RootCaCertificate ::= ExplicitCertificate (WITH COMPONENTS { ...,
  issuer (WITH COMPONENTS {self}),
  toBeSigned (WITH COMPONENTS { ...,
    id (WITH COMPONENTS {
      name ("v2xrootca.ghsiss.com")
    }),
    cracaId('000000'H),
    crlSeries(0),
    validityPeriod (WITH COMPONENTS { ...,
      duration (RootCaCertExpiration) – set to 70 years
    }),
    region ABSENT,
    assuranceLevel ABSENT,
    appPermissions (SequenceOfPsidSsp (SIZE(2)) (CONSTRAINED BY {
      PsidSsp (WITH COMPONENTS {
        psid (SecurityMgmtPsid),
        ssp --OER encoding of ScmsSsp indicating RootCaSsp
      }),
      PsidSsp (WITH COMPONENTS {
        psid (CrlPsid),
        ssp (WITH COMPONENTS {opaque(CONTAINING CrlSsp (WITH COMPONENTS {...,
          associatedCraca(isCraca),
          crls (PermissibleCrls (SIZE(1)) (CONSTRAINED BY {
            CrlSeries (ScmsSpclComponentCrlSeries)
          }))
        }))})
      })
    })),
    certIssuePermissions (SequenceOfPsidGroupPermissions (SIZE(4)) (CONSTRAINED BY {
      PsidGroupPermissions ( WITH COMPONENTS {...,
               subjectPermissions (WITH COMPONENTS {
          all
        }),
        minChainDepth(3),
        chainDepthRange(-1),
        eeType ({app, enrol})
      }),
      PsidGroupPermissions ( WITH COMPONENTS {...,
               subjectPermissions (WITH COMPONENTS{
          explicit (SequenceOfPsidSspRange (SIZE (1)) (WITH COMPONENT (WITH COMPONENTS {
            psid (SecurityMgmtPsid), sspRange ABSENT
          })))
        }),
        minChainDepth(1),
        chainDepthRange(-1),
               eeType ({app, enrol})
      }),
      PsidGroupPermissions ( WITH COMPONENTS {...,
               subjectPermissions (WITH COMPONENTS{
          explicit (SequenceOfPsidSspRange (SIZE (1)) (WITH COMPONENT (WITH COMPONENTS {
            psid (MisbehaviorReportingPsid), sspRange ABSENT
          })))
        }),
        minChainDepth(1),
        chainDepthRange(-1),
               eeType ({app, enrol})
      }),
      PsidGroupPermissions ( WITH COMPONENTS {...,
               subjectPermissions (WITH COMPONENTS{
          explicit (SequenceOfPsidSspRange (SIZE (1)) (WITH COMPONENT (WITH COMPONENTS {
            psid (CrlPsid), sspRange (WITH COMPONENTS {all})
          })))
        }),
        minChainDepth(1),
        chainDepthRange(-1),
               eeType ({app, enrol})
      })
    })),
    certRequestPermissions ABSENT,
    canRequestRollover ABSENT,
    encryptionKey ABSENT,
    verifyKeyIndicator (WITH COMPONENTS {
      verificationKey (WITH COMPONENTS {
        ecdsaNistP256 (WITH COMPONENTS {
          compressed-y-0, compressed-y-1
        })
      })
    })
  })
})
```

9.1.2 V2XRCA CRL Profile

```
IEEE1609dot2Crl {iso(1) identified-organization(3) ieee(111)
standards-association-numbered-series-standards(2) wave-stds(1609)
dot2(2) crl(3) protocol(2)}

DEFINITIONS AUTOMATIC TAGS ::= BEGIN

EXPORTS ALL;

IMPORTS

  Ieee1609Dot2Data
FROM IEEE1609dot2 {iso(1) identified-organization(3) ieee(111)
    standards-association-numbered-series-standards(2) wave-stds(1609)
    dot2(2) base (1) schema (1)}

  Opaque,
  Psid
FROM IEEE1609dot2BaseTypes {iso(1) identified-organization(3) ieee(111)
    standards-association-numbered-series-standards(2) wave-stds(1609)
    dot2(2) base(1) base-types(2)}

  CrlContents
FROM IEEE1609dot2CrlBaseTypes {iso(1) identified-organization(3) ieee(111)
    standards-association-numbered-series-standards(2) wave-stds(1609)
    dot2(2) crl(3) base-types(1)}

;

CrlPsid ::= Psid(256)

SecuredCrl ::= Ieee1609Dot2Data (WITH COMPONENTS {...,
  content (WITH COMPONENTS {
    signedData  (WITH COMPONENTS {...,
      tbsData (WITH COMPONENTS {
        payload (WITH COMPONENTS {...,
          data (WITH COMPONENTS {...,
             content (WITH COMPONENTS {
                unsecuredData (CONTAINING CrlContents)
            })
          })
        }),
        headerInfo (WITH COMPONENTS {...,
          psid (CrlPsid),
          generationTime ABSENT,
          expiryTime ABSENT,
          generationLocation ABSENT,
          p2pcdLearningRequest ABSENT,
          missingCrlIdentifier ABSENT,
          encryptionKey ABSENT
        })
      })
    })
  })
})


IEEE1609dot2CrlBaseTypes {iso(1) identified-organization(3) ieee(111)
standards-association-numbered-series-standards(2) wave-stds(1609)
dot2(2) crl(3) base-types(1)}

DEFINITIONS AUTOMATIC TAGS ::= BEGIN

EXPORTS ALL;

IMPORTS
  CrlSeries,
  GeographicRegion,
  HashedId8,
  HashedId10,
  IValue,
  LaId,
  LinkageSeed,
  Opaque,
  Psid,
  Signature,
  ThreeDLocation,
  Time32,
  Uint3,
  Uint8,
  Uint16,
  Uint32,
  ValidityPeriod
FROM IEEE1609dot2BaseTypes {iso(1) identified-organization(3) ieee(111)
    standards-association-numbered-series-standards(2) wave-stds(1609)
    dot2(2) base(1) base-types(2)}
;

--
--
--  CRL contents
--
--

CrlContents ::= SEQUENCE {
    version            Uint8 (1),
    crlSeries          CrlSeries,
    cracaId            HashedId8, - set to HashedId8 of V2XRCA cert
    issueDate          Time32,
    nextCrl            Time32,  - set to 5 years from issueDate
    priorityInfo       CrlPriorityInfo, - not used
    typeSpecific       CHOICE {
        fullHashCrl          ToBeSignedHashIdCrl,
        ...
    }
}

CrlSeries ::= 256

ToBeSignedHashIdCrl ::= SEQUENCE {
    crlSerial         Uint32,
    entries           SequenceOfHashBasedRevocationInfo,
    ...
}

HashBasedRevocationInfo ::= SEQUENCE {
    id         HashedId10,
    expiry     Time32
}

SequenceOfHashBasedRevocationInfo ::=
    SEQUENCE OF HashBasedRevocationInfo
```

9.2 AUC2XRCA Profile

The AUC2XRCA Root Certificate, CRL, and CTL shall materially conform to the ETSI standards. Examples are listed below.

9.2.1 AUC2XRCA Root Certificate Profile

```
{
   "version":3,
   "type":"explicit",
   "issuer":{
      "self":"sha256"
   },
   "toBeSigned":{
      "id":{
         "name":"AU C-ITS Root CA"
      },
      "cracaId":"000000",
      "crlSeries":0,
      "validityPeriod":{
         "start":494380805,
         "duration":{
            "years":8
         }
      },
      "region":{
         "identifiedRegion":[
            {
               "countryOnly":36
            }
         ]
      },
      "assuranceLevel":"00",
      "appPermissions":[
         {
            "psid":622,
            "ssp":{
               "bitmapSsp":"01"
            }
         },
         {
            "psid":624,
            "ssp":{
               "bitmapSsp":"0138"
            }
         }
      ],
      "certIssuePermissions":[
         {
            "subjectPermissions":{
               "all":null
            },
            "minChainLength":2,
            "eeType":"C0"
         },
         {
            "subjectPermissions":{
               "explicit":[
                  {
                     "psid":623,
                     "sspRange":{
                        "bitmapSspRange":{
                           "sspValue":"01FE",
                           "sspBitmask":"FF01"
                        }
                     }
                  }
               ]
            },
            "chainLengthRange":1,
            "eeType":"C0"
         }
      ],
      "verifyKeyIndicator":{
         "verificationKey":{
            "ecdsaNistP256":{
               "compressed-y-0":"EB83FDABAA100637D5699F5109B5AE84F6F6D1D3934B937936CA6F236CDC8B54"
            }
         }
      }
   },
   "signature":{
      "ecdsaNistP256Signature":{
         "rSig":{
            "x-only":"2460d15f31a4721799611ff192be24da3080ac48a963318a7d2ccc812a1c4709"
         },
         "sSig":"8235f7e4164e5b830d1b27ab71283857e569d7e9d39fdf63017d7be153441a49"
      }
   }
}
```

9.2.2 AUC2XRCA CRL Profile

9.2.2.1 CRL

```
{
   "protocolVersion":3,
   "content":{
      "signedData":{
         "hashId":"sha256",
         "tbsData":{
            "payload":{
               "data":{
                  "protocolVersion":3,
                  "content":{
                     "unsecuredData":"01840001011D83848521468F350100"
                  }
               }
            },
            "headerInfo":{
               "psid":622,
               "generationTime":495158405000000
            }
         },
         "signer":{
            "certificate":[
               {
                  "version":3,
                  "type":"explicit",
                  "issuer":{
                     "self":"sha256"
                  },
                  "toBeSigned":{
                     "id":{
                        "name":"AU C-ITS Root CA"
                     },
                     "cracaId":"000000",
                     "crlSeries":0,
                     "validityPeriod":{
                        "start":494380805,
                        "duration":{
                           "years":8
                        }
                     },
                     "region":{
                        "identifiedRegion":[
                           {
                              "countryOnly":36
                           }
                        ]
                     },
                     "assuranceLevel":"00",
                     "appPermissions":[
                        {
                           "psid":622,
                           "ssp":{
                              "bitmapSsp":"01"
                           }
                        },
                        {
                           "psid":624,
                           "ssp":{
                              "bitmapSsp":"0138"
                           }
                        }
                     ],
                     "certIssuePermissions":[
                        {
                           "subjectPermissions":{
                              "all":null
                           },
                           "minChainLength":2,
                           "eeType":"C0"
                        },
                        {
                           "subjectPermissions":{
                              "explicit":[
                                 {
                                    "psid":623,
                                    "sspRange":{
                                       "bitmapSspRange":{
                                          "sspValue":"01FE",
                                          "sspBitmask":"FF01"
                                       }
                                    }
                                 }
                              ]
                           },
                           "chainLengthRange":1,
                           "eeType":"C0"
                        }
                     ],
                     "verifyKeyIndicator":{
                        "verificationKey":{
                           "ecdsaNistP256":{
                                                                                        "compressed-y-
0":"EB83FDABAA100637D5699F5109B5AE84F6F6D1D3934B937936CA6F236CDC8B54"
                           }
                        }
                     }
                  },
                  "signature":{
                     "ecdsaNistP256Signature":{
                        "rSig":{
                           "x-only":"2460D15F31A4721799611FF192BE24DA3080AC48A963318A7D2CCC812A1C4709"
                        },
                        "sSig":"8235F7E4164E5B830D1B27AB71283857E569D7E9D39FDF63017D7BE153441A49"
                     }
                  }
               }
            ]
         },
         "signature":{
            "ecdsaNistP256Signature":{
               "rSig":{
                  "x-only":"839d682bdc684489be0fb4bd26cf4ac9176cb057b85eb281837825794577d5b6"
               },
               "sSig":"0021fe9841ae5b5fa410036f884ccd7a2ff8455681f6cac9ed012bbdbce0908b"
            }
         }
      }
   }
}
```

9.2.2.2 Inner CRL

```
{
  "version":1,
  "content":{
    "certificateRevocationList":{
      "version":1,
      "thisUpdate":495158405,
      "nextUpdate":558272309,
      "entries":[]
    }
  }
}
```

9.2.3 AUC2XRCA CTL Profile

9.2.3.1 CTL

```
{
   "protocolVersion":3,
   "content":{
      "signedData":{
         "hashId":"sha256",
         "tbsData":{
            "payload":{
               "data":{
                  "protocolVersion":3,
                  "content":{
                     "unsecuredData":"018600010121468F35FF01010380818080030080AA9B82A72933269279811965
612E70726F642E61752E6332782E697373636D732E636F6D00000000001D7CED058600058301018000240001018002026F8103
02010E01020081008001018002026F82060201C002FFFF00808399F8364B772B7514A59E5394CDB158F84C6222C064B3C41F8E
59FAB9DE7094AA808082A62070C399B1F2C781717A45AF93B53537E4C6008F620ED3AE6A8B42AA825BE08080E05EF1154B6FBF
5F51C6ABA9C45F42E26C3AB7911DBA0A546D79F4DF379904BE77F2E9105F817C5F02E834DFD1BD11CD48919C0619565B4C53A4
B4E58598C8A04068747470733A2F2F65612E70726F642E61752E6332782E697373636D732E636F6D2F76616C69646174652D61
7574686F72697A6174696F6E2D72657175657374442687474470733A2F2F65612E70726F642E61752E6332782E697373636D732E
636F6D2F70726F766973696F6E2D656E726F6C6C6D656E742D6365727469666963617465808280030080AA9B82A72933269279
811961612E70726F642E61752E6332782E697373636D732E636F6D00000000001D7CED05860005830101800024000101800202
6F81030201320101008100808336157CB2D4405C1ED7D3CC0150DCC63DB690D16EBD22C4BE797D54DC7E950A678080822828B3
BE70C4D5C66DE29F07CD5FCF34B08C9213B41D0D8C71E0E7C02843DC2E80800717E16A172584611E0C1F543670D2F01190F552
E036D93E23A9FC24C32BEDB6C6CB85A29033F50F2741D00BA1AD6A1DEBC08787A2D8114B529CD6DDFECC8A174068747470733A
2F2F61612E70726F642E61752E6332782E697373636D732E636F6D2F70726F766973696F6E2D617574686F72697A6174696F6E
2D7469636B657480832168747470733A2F2F64632E70726F642E61752E6332782E697373636D732E636F6D0101AA9B82A72933
2692"
                  }
               }
            },
            "headerInfo":{
               "psid":624,
               "generationTime":495158405000000
            }
         },
         "signer":{
            "certificate":[
               {
                  "version":3,
                  "type":"explicit",
                  "issuer":{
                     "self":"sha256"
                  },
                  "toBeSigned":{
                     "id":{
                        "name":"AU C-ITS Root CA"
                     },
                     "cracaId":"000000",
                     "crlSeries":0,
                     "validityPeriod":{
                        "start":494380805,
                        "duration":{
                           "years":8
                        }
                     },
                     "region":{
                        "identifiedRegion":[
                           {
                              "countryOnly":36
                           }
                        ]
                     },
                     "assuranceLevel":"00",
                     "appPermissions":[
                        {
                           "psid":622,
                           "ssp":{
                              "bitmapSsp":"01"
                           }
                        },
                        {
                           "psid":624,
                           "ssp":{
                              "bitmapSsp":"0138"
                           }
                        }
                     ],
                     "certIssuePermissions":[
                        {
                           "subjectPermissions":{
                              "all":null
                           },
                           "minChainLength":2,
                           "eeType":"C0"
                        },
                        {
                           "subjectPermissions":{
                              "explicit":[
                                 {
                                    "psid":623,
                                    "sspRange":{
                                       "bitmapSspRange":{
                                          "sspValue":"01FE",
                                          "sspBitmask":"FF01"
                                       }
                                    }
                                 }
                              ]
                           },
                           "chainLengthRange":1,
                           "eeType":"C0"
                        }
                     ],
                     "verifyKeyIndicator":{
                        "verificationKey":{
                           "ecdsaNistP256":{
                                                                                        "compressed-y-
0":"EB83FDABAA100637D5699F5109B5AE84F6F6D1D3934B937936CA6F236CDC8B54"
                           }
                        }
                     }
                  },
                  "signature":{
                     "ecdsaNistP256Signature":{
                        "rSig":{
                           "x-only":"2460D15F31A4721799611FF192BE24DA3080AC48A963318A7D2CCC812A1C4709"
                        },
                        "sSig":"8235F7E4164E5B830D1B27AB71283857E569D7E9D39FDF63017D7BE153441A49"
                     }
                  }
               }
            ]
         },
         "signature":{
            "ecdsaNistP256Signature":{
               "rSig":{
                  "x-only":"fb2c4dcd5e3ad8e39433f75d93d57eb5ed357a1c494e510c736f98e367384fea"
               },
               "sSig":"49067acb26bb06947ad47582ffb3b6058ce5d06b81150dd9648408bd779b869f"
            }
         }
      }
   }
}
```

9.2.3.2 Inner CTL

```
{
  "version": 1,
  "content": {
    "certificateTrustListRca": {
      "version": 1,
      "nextUpdate": 558272309,
      "isFullCtl": true,
      "ctlSequence": 1,
      "ctlCommands": [
        {
          "add": {
            "ea": {
              "eaCertificate": {
                "version": 3,
                "type": "explicit",
                "issuer": {
                  "sha256AndDigest": "AA9B82A729332692"
                },
                "toBeSigned": {
                  "id": {
                    "name": "ea.prod.au.c2x.isscms.com"
                  },
                  "cracaId": "000000",
                  "crlSeries": 0,
                  "validityPeriod": {
                    "start": 494726405,
                    "duration": {
                      "years": 5
                    }
                  },
                  "region": {
                    "identifiedRegion": [
                      {
                        "countryOnly": 36
                      }
                    ]
                  },
                  "assuranceLevel": "00",
                  "appPermissions": [
                    {
                      "psid": 623,
                      "ssp": {
                        "bitmapSsp": "010E"
                      }
                    }
                  ],
                  "certIssuePermissions": [
                    {
                      "subjectPermissions": {
                        "all": null
                      }
                    },
                    {
                      "subjectPermissions": {
                        "explicit": [
                          {
                            "psid": 623,
                            "sspRange": {
                              "bitmapSspRange": {
                                "sspValue": "01C0",
                                "sspBitmask": "FFFF"
                              }
                            }
                          }
                        ]
                      }
                    }
                  ],
                  "encryptionKey": {
                    "supportedSymmAlg": "aes128Ccm",
                    "publicKey": {
                      "eciesNistP256": {
                                                                                       "compressed-y-1":
"99F8364B772B7514A59E5394CDB158F84C6222C064B3C41F8E59FAB9DE7094AA"
                      }
                    }
                  },
                  "verifyKeyIndicator": {
                    "verificationKey": {
                      "ecdsaNistP256": {
                                                                                     "compressed-y-0":
"A62070C399B1F2C781717A45AF93B53537E4C6008F620ED3AE6A8B42AA825BE0"
                      }
                    }
                  }
                },
                "signature": {
                  "ecdsaNistP256Signature": {
                    "rSig": {
                      "x-only": "E05EF1154B6FBF5F51C6ABA9C45F42E26C3AB7911DBA0A546D79F4DF379904BE"
                    },
                    "sSig": "77F2E9105F817C5F02E834DFD1BD11CD48919C0619565B4C53A4B4E58598C8A0"
                  }
                }
              },
              "aaAccessPoint": "https://ea.prod.au.c2x.isscms.com/validate-authorization-request",
              "itsAccessPoint": "https://ea.prod.au.c2x.isscms.com/provision-enrollment-certificate"
            }
          }
        },
        {
          "add": {
            "aa": {
              "aaCertificate": {
                "version": 3,
                "type": "explicit",
                "issuer": {
                  "sha256AndDigest": "AA9B82A729332692"
                },
                "toBeSigned": {
                  "id": {
                    "name": "aa.prod.au.c2x.isscms.com"
                  },
                  "cracaId": "000000",
                  "crlSeries": 0,
                  "validityPeriod": {
                    "start": 494726405,
                    "duration": {
                      "years": 5
                    }
                  },
                  "region": {
                    "identifiedRegion": [
                      {
                        "countryOnly": 36
                      }
                    ]
                  },
                  "assuranceLevel": "00",
                  "appPermissions": [
                    {
                      "psid": 623,
                      "ssp": {
                        "bitmapSsp": "0132"
                      }
                    }
                  ],
                  "certIssuePermissions": [
                    {
                      "subjectPermissions": {
                        "all": null
                      }
                    }
                  ],
                  "encryptionKey": {
                    "supportedSymmAlg": "aes128Ccm",
                    "publicKey": {
                      "eciesNistP256": {
                                                                                     "compressed-y-1":
"36157CB2D4405C1ED7D3CC0150DCC63DB690D16EBD22C4BE797D54DC7E950A67"
                      }
                    }
                  },
                  "verifyKeyIndicator": {
                    "verificationKey": {
                      "ecdsaNistP256": {
                                                                                     "compressed-y-0": 
"2828B3BE70C4D5C66DE29F07CD5FCF34B08C9213B41D0D8C71E0E7C02843DC2E"
                      }
                    }
                  }
                },
                "signature": {
                  "ecdsaNistP256Signature": {
                    "rSig": {
                      "x-only": "0717E16A172584611E0C1F543670D2F01190F552E036D93E23A9FC24C32BEDB6"
                    },
                    "sSig": "C6CB85A29033F50F2741D00BA1AD6A1DEBC08787A2D8114B529CD6DDFECC8A17"
                  }
                }
              },
              "accessPoint": "https://aa.prod.au.c2x.isscms.com/provision-authorization-ticket"
            }
          }
        },
        {
          "add": {
            "dc": {
              "url": "https://dc.prod.au.c2x.isscms.com",
              "cert": [
                "AA9B82A729332692"
              ]
            }
          }
        }
      ]
    }
  }
}
```

9.3 V2X Elector Profiles

The V2X Elector Certificate Profile and CTL Profile shall materially conform to IEEE 1609.2-2016 as profiled by the IPA and approved by SCMS Manager. The required profiles are specified in the following sections.

9.3.1 V2X Elector Certificate Profile

9.3.1.1 ToBeSigned

```
{
  "id": {
    "name": <CertificateId>
  },
  "cracaId": "000000",
  "crlSeries": 0,
  "validityPeriod": {
    "start": <Start Time32>,
    "duration": {
      "years": <Duration Years>
   }
  },
  "appPermissions": [
    {
      "psid": 35,
      "ssp": {
        "opaque": "800002"
      }
    }
  ],
  "verifyKeyIndicator": {
    "verificationKey": {
      "ecdsaNistP384": {
        ( "compressed-y-0": <48 Byte HEX key>
                   OR
    "compressed-y-1": <48 Byte HEX key> )
      }
    }
  }
}
```

9.3.1.2 Certificate

```
{
  "version": 3,
  "type": "explicit",
  "issuer": {
    "self": "sha384"
  },
  "toBeSigned": {
    <ToBeSignedCertificate>
  },
  "signature": {
    "ecdsaNistP384Signature": {
      "rSig": {
        "x-only": <Signature R Component>
      },
      "sSig": <Signature S Component>
    }
  }
}
```

9.3.2 V2X CTL Profile

```
{
  "version": 2,
  "content": {
    "cert": {
      "multiSignedCertificateTrustList": {
        "type": 1,
        "tbsCtl": {
          <FullIeeeTbsCtl>
        },
        "unsigned": [
          <Elector Certificate 1>,
          <Elector Certificate 2>,
          <Elector Certificate 3>,
          <Elector Certificate 4>,
          <Elector Certificate 5>,
          <ISS Root Certificate>
        ],
        "signatures": [
          <Elector CtlSignature 1>
          <Elector CtlSignature 2>
          <Elector CtlSignature 3>
          <Elector CtlSignature 4>
          <Elector CtlSignature 5>
        ]
      }
    }
  }
}
```

10 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The policies in this CP are designed to meet or exceed the requirements of the AICPA/CICA WebTrust Program for Certification Authorities.

10.1 Frequency of Assessment

On at least an annual basis, ISS shall retain an independent auditor who shall assess its compliance with this CP and its CPS according to WebTrust for Certification Authorities principles and criteria.

10.2 Auditor’s Relationship to Assessed Entity

ISS shall utilize an independent auditor accredited to audit according to AICPA/CICA WebTrust for Certification Authorities principles and criteria.

10.3 Topics Covered by Assessment

The audit must conform to WebTrust standards and cover the ISS’ compliance with its business practices, CP, CPS, and evaluate the integrity of the IRCA’s PKI operations.

10.4 Actions Taken as a Result of Deficiency

For any deficiency identified as a result of an audit, the IPA will determine its significance and will specify the required remediation requirements. The IPA is responsible for ensuring that any such remediation efforts are completed in a timely manner.

10.5 Communication of Results

Audit results shall be communicated to the IPA and ISS Executive Management.

10.6 Self-Audits

ISS may perform self-audits as it determines necessary or as directed by the IPA.

11 MISCELLANEOUS

11.1 Representations and Warranties

11.1.1 CA Representations and Warranties

ISS represents that it and the IRCA systems shall comply, in all material aspects, with this CP, the CPS, its internal and published policies and procedures, and all applicable laws and regulations. ISS expressly disclaims all other representations and warranties express or implied.

11.1.2 Subscriber Representations and Warranties

Subscriber is solely responsible for any representations or warranties it makes to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. As a pre-condition to being issued a Certificate, each Subscriber represents and warrants that it shall:

1. Properly use a FIPS 140-2 Level 3 validated HSM to securely generate and protect its subordinate CA Private Keys from compromise;
2. Submit its CP and CPS to the IPA for approval (Such approval shall not be unreasonably withheld);
3. Use the ISS End Entity Attestation to verify that Subscriber's customers have well-constructed devices with sufficient security controls to protect the V2X ecosystem;
4. Only issue certificates from its V2X CMS or C2X CMS to end entities conforming to the then current related end entity security requirements as published by US-DOT, SCMS Manager, ICAB or IPA. In the event of a conflict among these documents, USDOT followed by SCMS Manager followed by the IPA shall prevail for the V2XRCA and the V2X Electors. ICAB followed by the IPA shall prevail for the AUC2XRCA;
5. Always communicate accurate and complete information to ISS;
6. Confirm the accuracy of Certificate data prior to using the Certificate;
7. Promptly cease using a Certificate and notify ISS if (i) any information that was submitted to ISS or is included in a Certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the Certificate;
8. Use the Certificate only for authorized and legal purposes, consistent with this CP, the CPS and the relevant Subscriber Agreement;
9. Abide by the Subscriber Agreement and this CP when requesting or using a Certificate; and
10. Promptly cease using the Certificate and related Private Key upon the Certificate's expiration.

11.2 Trademarks

WebTrust is a trademark of the Canadian Institute of Chartered Accountants (http://www.cica.ca).

All other cited trade names and marks are property of their respective owners.

11.3 Waivers

The IPA, at its sole discretion, may grant a written waiver to portions of this Certificate Policy to a Subscriber.

12 CONTACT

The Contact Information for CP related correspondence:

INTEGRITY Security Services Policy Authority
30 W Sola Street
Santa Barbara, CA 93101
Phone: (888) 951-4477
Email: iss.policyauthority@ghsiss.com

Support Contact (24x7 Ticketing System):

ISS CMS / SCMS IRCAs including V2X Elector, V2XRCA, & AUC2XRCA:
support@isscms.com

Other IRCAs: support@ghsiss.com

IRCA publications are available here:

https://ghsiss.com/root-ca

13 VERSION HISTORY

Version	Date	Comments
1.0	March 21, 2016	Initial release
1.1	October 5, 2016	Added TOC. Added new definitions. Updated Profiles for SCMS 1.1. Added notification clarifications for enrollment, revocation, and key changes. Clarified transition of the Root in the event of service termination by ISS. Modified for WebTrust.
1.2	September 12, 2019	Generalized CP to cover additional root CAs, including the AUC2XRCA. Added end entity security requirements to Subscriber Representations. Clarified CRL issuance time period following a disaster at the primary site.
1.3	December 10, 2019	Added support for Electors
1.4	March 27, 2023	Added support for ISO-15118 V2G root certificates