Aviareto

Certification Practice Statement

Version 1.4

Status: Original

Version: 1.4

Date: 10 February 2006

1. Introduction

1.1. Overview

This Certification Practice Statement (CPS) describes the practices relating to all certificate lifecycle services (e.g. issuance, management, revocation, and renewal) that Aviareto Limited (Aviareto) employs as the Registrar for the Registry under the Convention on International Interests in Mobile Equipment (Convention), Protocol to the Convention on matters specific to Aircraft Equipment (Protocol) and the Regulations for the International Registry (Regulations). For the purposes of the Registry, Aviareto has established a managed PKI service for the management of digital certificates.

The format of this document follows the "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" (RFC3647, Nov2003) published by IETF (Internet Engineering Task Force) (X.509). Aviareto recommends that users review the acronyms and definitions in section 1.6 prior to reading this document.

Save as otherwise provided, terms used in this CPS have the same meanings as they have in the Procedures and the Terms and Conditions.

1.2. Document Name and Identification

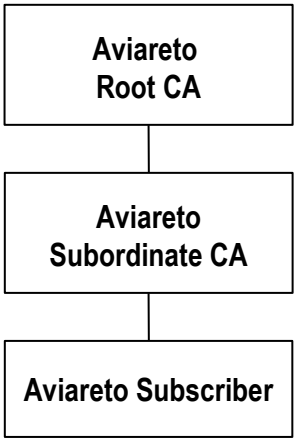
This document is the Aviareto Certification Practice Statement (CPS) and provides certificate policies specifically for the management of digital certificates in the Registry.

1.3. PKI Participants

1.3.1. Certification Authorities

The certification authority (CA) authorized to issue certificates under this CPS is Aviareto. The CA supports the creation of public key certificates for use in the Registry. The CA makes use of a Managed PKI Private Label Service operated by VeriSign.

The following diagram shows the CA hierarchy:



1.3.2. Registration Authorities

A registration authority (RA) entity performs identification and authentication of certificate applicants.

The RA entities are:

- in respect of Administrators, Aviareto; and
- in respect of other Registry Users, their Registry User Entity's Administrator.

1.3.3. Subscribers

There are three levels of subscribers for this service. These include:

1. The Registrar and its representatives;
2. Administrators; and
3. other Registry Users.

1.3.4. Relying Parties

A relying party is any entity that relies on a certificate issued by Aviareto. The Registrar is the only relying party.

1.3.5. Other Participants

Aviareto acts as CA only in its capacity as Registrar, and the certificates issued are only for use in connection with the Registry. There are no other participants in this certification scheme.

1.4. Certificate Usage

1.4.1. Acceptable Application

Registry Users shall only use certificates issued under this CPS for:

- the purposes of providing client authentication to the Registry; and

- the purpose of providing electronic signatures in accordance with the Convention, Protocol, Regulations, Procedures and the Terms and Conditions.

The Registrar shall only use certificates issued under this CPS for:

- the purposes of signing search certificates; and
- the purpose of signing the activity log.

1.4.2. Prohibited Application

Registry Users shall not use any certificate issued under this CPS:

- for the purpose of providing authentication to parties not being the Registrar;
- for the purpose of providing electronic signatures other than in accordance with the Convention, Protocol, Regulations, Procedures and the Terms and Conditions;
- for any export, import, use or activity that contravenes applicable law;
- in conjunction with illegal activities;
- for personal use or purposes not related to the Registry;
- after it has been revoked; or
- for any use not expressly permitted in subsection 1.4.1.

1.5. Policy Administration

1.5.1. Administration Organisation

The administration organisation for the purposes of this CPS is Aviareto Limited (a company incorporated in the Republic of Ireland), Regus House, Harcourt Centre, Harcourt Road, Dublin 2, Ireland. (www.aviareto.aero)

1.5.2. Contact Person

The contact person for the purposes of this CPS is Aviareto's operations director, who can be contacted care of "registryofficials@aviareto.aero".

1.6. Definitions and Acronyms

1.6.1. Definitions

In this CPS the following terms shall have the meanings given:

***Aviareto RA Component*:** The software component that is responsible for sending certificate requests to the *Aviareto Subordinate CA* and receiving certificates from the *Aviareto Subordinate CA*.

***Aviareto RA Operator*:** An individual appointed by Aviareto to act as the Registration Authority official responsible for approving Administrators.

Aviareto Root CA: The Aviareto CA that issued the Aviareto Subordinate CA certificate, positioned on the top of the CA hierarchy.

Aviareto Subordinate CA: The Aviareto CA that issues certificates to all Registry Users.

Certificate Applicant: Any person that has applied for a certificate from Aviareto.

Certificate Revocation List: A list containing certificates that have been revoked prior to their expiration. This list is periodically published by the CA.

***Distinguished Name*:** means the distinguished named associated with a certificate that is in accordance with X.501.

***Terms and Conditions*:** The INTERNATIONAL REGISTRY FOR INTERNATIONAL INTERESTS IN MOBILE EQUIPMENT (AIRCRAFT EQUIPMENT) TERMS AND CONDITIONS OF USE, as the same are constituted from time to time, available via www.internationalregistry.aero.

VeriSign CPS: the VeriSign CPS, available via https://www.verisign.com/repository/CPS/, the current version of which is Version 3.0, effective date April 1, 2005.

1.6.2. Acronyms

CA: Certification Authority

CP: Certificate Policy

CPS: Certification Practice Statement

CRL: Certificate Revocation List

DN: Distinguished Name

HSM: Hardware Security Module

JKS: Java Key Store

OCSP: Online Certificate Status Protocol

PKI: Public Key Infrastructure

RA: Registration Authority

SSL: Secure Socket Layer

URL: Uniform Resource Locator

2. Publication and Repository

2.1. Publication of Aviareto Information

Upon revocation of a Registry User certificate, Aviareto publishes notice of such revocation in the Certificate Revocation List (CRL).

2.2. Availability of Aviareto Information

Aviareto shall make available certificate revocation information by publishing a Certificate Revocation List (CRL) in the following location:

URI=http://onsitecrl.verisign.com/AviaretoLtdInternationalRegistryCA/LatestCRL.crl

2.3. Frequency of Publication

The Certificate Revocation List (CRL) shall be updated every 24 hours.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

All Registry Users require a Distinguished Name. The Distinguished Name will appear in the certificate subject field.

The following table (1) specifies the Distinguished Names of the *Aviareto Root CA* certificate:

DN Attribute	Value
Country	IE
Organisation	Aviareto Limited
Common Name	Aviareto Root CA

Table 1

The following table (2) specifies the Distinguished Names of the Aviareto Subordinate CA certificate:

DN Attribute	Value
Country	IE
Organisation	Aviareto Limited
Common Name	International Registry CA

Table 2

The following table (3) specifies the Distinguished Names of the Registry User certificates:

DN Attribute	Value
Organisation	Registry User Entity
Organisational Unit	Registry User's department (will

	determine role)
Common Name	*This unique ID is dynamically generated by the Registry application and take the format <Company name> - <Username> - <User ID>*

Table 3

The following table (4) specifies the Distinguished Names of the Aviareto Registry certificates:

DN Attribute	Value
Organisation	Subscriber's organisation
Organisational Unit	Subscriber's department (will determine role)
Common Name	*This unique ID is dynamically generated by the Registry application and takes the format* Aviareto – *Username> - <User ID>*

Table 4

3.1.2. Need for Names to be Meaningful

Registry User Distinguished Names must be meaningful. The Distinguished Names must have an association with the name of the relevant Registry User Entity and each Distinguished Name must uniquely identify the Registry User.

3.1.3. Anonymous or Pseudonymous Subscribers

Anonymous or pseudonymous Registry Users are not permitted.

3.1.4. Name Uniqueness

Registry User Distinguished Names must be unique. Certificate applications that contain a Distinguished Name that does not sufficiently distinguish the *Certificate Applicant* from an existing Registry User will be rejected.

3.1.5. Recognition, Authentication and Role of Trade Marks

Aviareto has no obligation to investigate or seek evidence in relation to a *Certificate Applicant's* ownership of or right to use any trade or service mark or any other right to use any name prior to certificate issuance.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Certificate Applicants must sign application data (which includes their own public key) using the corresponding private key in order to create a self-signed certificate. Aviareto will ensure by verification of the signature that the *Certificate Applicant* demonstrates the possession of the private key.

3.2.2. Authentication of Organisation Identity

The *Aviareto RA Operator* will only process certificate requests from *Certificate Applicants* that want to become an Administrator.

In order for an organisation to become a Registry User Entity, that organisation and its proposed administrator must be approved in accordance with the Regulations and Procedures..

3.2.3. Authentication of Individual Identity

In respect of proposed Registry Users other than Administrators, the *Aviareto RA Component* will only process certificate requests from *Certificate Applicants* that have been approved by the relevant Registry User Entity's Administrator in accordance with the Regulations and Procedures.

The applicant must provide the following mandatory information:

- *Certificate Applicant* name;
- Registry User Entity name; and
- email address.

The *Certificate Applicant* must accept the Terms and Conditions and provide payment details.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Routine Re-Key Identification and Authentication

A request for Re-key will be treated as an initial certificate application as per the provisions of section 3.2.3

3.3.2. Re-Key after Revocation Identification and Authentication

A request for Re-key after revocation will be treated as an initial certificate application as per the provisions of section 3.2.3

3.4. Identification and Authentication for Revocation Requests

The *Aviareto RA Operator* shall be responsible for approving certificate revocation requests for Administrators' certificates.

The Administrator shall be responsible for approving certificate revocation requests for other Registry Users' certificates.

4. Certificate Life-Cycle Operational Requirements

All certificates issued under this CPS will expire one year after being issued.

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Proposed Administrators and Registry Users can submit certificate applications, in accordance with the Procedures.

4.1.2. Enrolment Process

4.1.2.1.Registry User Enrolment

All *Certificate Applicants* applying to become Registry Users must be approved in accordance with the Procedures and complete the following procedure for each certificate application:

- generate a key-pair using the applet provided by the Registry;
- complete the Registry User registration form;
- demonstrate possession of the private key by using it to sign application data (including the corresponding public key), in order to create a self-signed certificate; and
- accept the Terms and Conditions.

4.1.2.2.Administrator Enrolment

All *Certificate Applicants* applying to become Administrators must be approved in accordance with the Procedures and complete the following procedure for each certificate application:

- generate a key-pair using the applet provided by the Registry;
- complete the Administrator registration form;
- demonstrate possession of the private key by using it to sign application data (including the corresponding public key), in order to create a self-signed certificate; and
- accept the Terms and Conditions.

4.2. Certificate Application Processing

4.2.1. Identification and Authentication Procedures

Certificate Applicants applying to become Registry Users must be approved by their Registry User Entity's Administrator in accordance with the Procedures. The Administrator is responsible for verifying the identity of the *Certificate Applicant*.

Certificate Applicants applying to become Administrators must be approved by Aviareto, acting through the *Aviareto RA Operator*.

4.2.2. Certificate Approval Criteria

The *Aviareto RA Component* will process a certificate application from a *Certificate Applicant* applying to become a Registry User if the application has been approved by the relevant Administrator and all criteria set out in section 3.2.3 are met.

The *Aviareto RA Operator* will approve a certificate application from a proposed Administrator if such proposed Administrator is approved by Aviareto in accordance with the Procedures and all criteria set out in section 3.2.2 are met.

4.2.3. Time Limit of Certificate Application Processing

Certificate Applicants have a maximum of 30 calendar days to complete the approval process. If, due to capacity constraints, Aviareto is unable to process certificate applications within this deadline, Aviareto may elect to extend this period of time and will endeavour to notify *Certificate Applicants* accordingly.

4.3. Certificate Issuance

4.3.1. CA Actions

The *Aviareto Subordinate CA* will issue a certificate following receipt of the *Aviareto RA Component* certificate issuance request.

4.3.2. Notification Mechanisms

An email is sent by the Registry to the *Certificate Applicant* notifying the *Certificate Applicant* of the certificate issuance. The email includes the URL at which the *Certificate Applicant* can pick up his certificate.

4.4. Certificate Acceptance

4.4.1. Applicant Conduct Constituting Certificate Acceptance

Registry Users are not required expressly to indicate acceptance of their Aviareto certificates. Failure of the Registry User to object to the certificate or its contents constitutes acceptance by the Registry User of the certificate.

4.4.2. Certificate Publication by the CA

Not applicable.

4.4.3. Notification of Certificate Issuance by the CA to other Entities

The Registry will receive notification of issued certificates.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Responsibilities

Use of the private key and certificate are subject to the Terms and Conditions. The Registry User shall use the private key and certificate only within the Registry as set out in Section 1.4.1.

In the event of compromise of the Registry User's private key the Registry User must, where required by Section 6(d) of the Procedures, request that the corresponding certificate be revoked.

4.5.2. Relying Party Responsibilities Relating to Subscriber's Public Key and Certificate

Certificates issued under this CPS must only be used within the Registry as set out in section 1.4.1. The Registry will not recognize revoked or expired certificates.

4.6. Certificate Renewal

Certificate renewal is the process of issuance of a new certificate to a subscriber without changing the subscriber public key or any other information in the certificate.

This is not supported by Aviareto. (see www.internationalregistry.aero)

4.7. Certificate Re-Key

Certificate Re-key is the process of a Registry User's generating a new key pair and applying for the issuance of a new certificate that certifies the new public key.

4.7.1. Circumstances for Certificate Re-key

A Registry User may request a certificate Re-key after the original certificate has expired or after the original certificate has been revoked for reasons of key compromise.

4.7.2. Who may Request Certificate Re-key

Any Registry User with an expired or revoked certificate

4.7.3. Procedures for Processing Re-key Requests

The request for certificate Re-key will be treated as an initial certificate application as per the provisions of section 3.2.3

4.7.4. Subscriber Notification of New Certificate

The certificate notification mechanism is in accordance with section 4.3.2

4.7.5. Conduct Constituting Acceptance of Certificate

The conduct constituting acceptance of the certificate is in accordance with section 4.4.1

4.7.6. Publication of Re-key Certificate by the CA

Not Implemented

4.7.7. Notification of Certificate Issuance to Other Entities

Not Implemented

4.8. Certificate Modification

Certificate modification is the process related to the issuance of a new certificate due to changes in the information in the certificate other than the subscriber public key.

This is not supported by Aviareto. If any certificate information changes it will be treated as a new certificate request and a new key pair generated by the *Certificate Applicant*.

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

An Administrator must revoke a certificate if to its actual knowledge:

- the private key corresponding to the certificate has been compromised and that is expected to result in unauthorised registrations;
- the Registry User does not comply with the Terms and Conditions or with this CPS;
- the certificate details are no longer valid; or
- the private key of the *Aviareto Root CA* or the *Aviareto Subordinate CA* has been compromised and that is expected to result in unauthorised registrations.

4.9.2. Who can request revocation

Registry Users other than Administrators can request the revocation of their own certificates by contacting their Administrator. A Registry User Entity's Administrator is responsible for revocation of that Registry User Entity's other Registry Users' certificates in accordance with 4.9.1.

Administrators can request the revocation of their own certificates by contacting the *Aviareto RA Operator.*

The *Aviareto RA Operator* can revoke an Administrator's certification:

(i) when requested to do so by the security officer or CFO of the Registry User Entity;

(ii) where in its view, there is a material risk of fraudulent registrations or other misuse; or

(iii) otherwise in accordance with the Procedures.

4.9.3. Procedure for revocation request

A Registry User must communicate any request for the revocation of his own certificate by contacting the Administrator of the Registry User Entity which he represents. Each Registry User Entity is responsible for managing the revocation of certificates issued to its Registry Users.

An Administrator must communicate any request for revocation of his own certificate by contacting the *Aviareto RA Operator* by telephone using the published telephone number, and the Administrator must confirm this telephone call by replying to an email sent from the *Aviareto RA Operator* to the Administrator.

4.9.4. Revocation request grace period

A Registry User must request the revocation of his certificate where required by Section 6(d) of the Procedures.

4.9.5. Time within which CA must process the revocation request

Aviareto shall use reasonable endeavours to process all revocation requests submitted to it without delay.

4.9.6. Revocation checking requirement for relying parties

The Registrar is the only relying party.

The Registrar will verify each Registry User's certificate by checking its status against the most recent CRL issued by the *Aviareto Subordinate CA*, and in addition the Registry internal CRL. This internal CRL contains a list of all certificates that have been revoked by the *Registry* since the most recent CRL was published.

4.9.7. CRL issuance frequency

The CRL of the Aviareto Subordinate CA is updated at least every 24 hours.

4.9.8. Maximum latency for CRLs (if applicable)

The CRL shall be published within minutes of generation.

4.9.9. On-line revocation/status checking availability

Not Implemented

4.9.10. On-line revocation checking requirements

Not Implemented

4.9.11. Other forms of revocation advertisements available

Not implemented

4.9.12. Special requirements re key compromise

Not Applicable

4.9.13. Certificate Suspension

Certificate suspension is not supported by Aviareto

4.10. Certificate status services

4.10.1. Operational characteristics

The Registrar will check the validity status of each Registry User certificate issued under this CPS relied upon by the Registrar using the latest CRL available and in addition the Registry internal CRL. This internal CRL contains a list of all certificates that have been revoked by the Registry since the most recent CRL was published. CRLs are available through a URL as specified in section 2.2.

4.10.2. Service availability

Services for certificate status are normally available without interruption 24x7.

4.10.3. Optional features

No optional features are implemented.

4.11. End of subscription

End of subscription occurs when the Registry User certificate has expired or has been revoked.

4.12. Key escrow and recovery

Aviareto does not support private key escrow.

5. Facilities, Management, and Operational Controls

For Certification Authority physical, procedural and personnel controls, please refer to the *VeriSign CPS*.

6. Technical Security Controls

For Certification Authority technical security controls, please refer to the *VeriSign CPS*.

6.1. Key pair generation and installation

6.1.1. Key pair generation

The *Aviareto RA Component* key pair will be generated in accordance with the documented VeriSign procedure for automated administration servers.

6.1.2. Private key delivery to the Registry User

All Registry Users will generate their private keys locally.

6.1.3. Public key delivery to certificate issuer

All Registry Users must submit their self-signed public keys to the *Aviareto RA Component*. The *Aviareto RA* will sign the approved requests and forward them to the *Aviareto Subordinate CA*.

6.1.4. CA public key delivery to relying parties

The Registrar is the only relying party and it will have the *Aviareto Subordinate CA* as well as the *Aviareto Root CA* certificate (which includes the Aviareto CA public key) pre-installed.

6.1.5. Key sizes

Key sizes are listed in table 5 below:

Aviareto Root CA	2048-bit
Aviareto Sub CA	1024-bit
Aviareto RA Component	1024-bit
Aviareto RA Operator	1024-bit
Registry Users	1024-bit

Table 5

6.1.6. Public key parameters generation and quality checking

Not Applicable

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

The *Aviareto Root CA* private key will only be used for issuance of the *Aviareto Subordinate CA* certificate and for CRL signing. The *Aviareto Subordinate CA* private key will only be used for certificate signing and CRL signing.

The Registry User's private key will only be used for the purposes of providing SSL client authentication to the web server hosting the *Registry* web pages and for the purpose of providing electronic signatures in accordance with the Terms and Conditions.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

Please refer to the *VeriSign CPS* for cryptographic module standards and controls relating to the *Aviareto Subordinate CA* and *Aviareto Root CA*.

The *Aviareto RA Component* private key is hardware based and is stored in a VeriSign provided HSM.

The Registry User's private key is software based and is stored in a JKS keystore. Registry Users must take all reasonable precautions to prevent the loss, disclosure, modification, or unauthorized use of their private keys.

6.2.2. Private Key (m out of n) multi-person control

Please refer to the *VeriSign CPS* for private key multi-person control relating to the *Aviareto Subordinate CA* and *Aviareto Root CA*.

The *Aviareto RA Component* requires only one person to activate it.

6.2.3. Private Key escrow

None of the private keys are escrowed.

6.2.4. Private Key backup

The Aviareto CA private keys are backed up for disaster recovery purposes as specified in the *VeriSign CPS*.

Registry User private keys are not backed up. The private key is installed on the Registry User's workstation. The private key may not be exported or copied to more than one workstation by the Registry User. Since the certificate will only be used for authentication and signing, there is no need for private key backup. In the event of a certificate being lost or destroyed, a new certificate can be supplied in accordance with this CPS.

6.2.5. Private Key archival

The *Aviareto CA* private keys are archived as specified in the *VeriSign CPS*. The *Aviareto RA Component*, *Aviareto RA Operator* and Registry User private keys are not archived.

6.2.6. Private Key transfer into or from a cryptographic module

Aviareto CA private keys shall be transferred between cryptographic modules as specified in the *VeriSign CPS*.

6.2.7. Private Key storage on cryptographic module

Aviareto CA private keys shall be stored as specified in the *VeriSign CPS*.

The *Aviareto RA Component* private key is stored in an encrypted form.

6.2.8. Method of activating Private Key

Aviareto CA private keys shall be activated as specified in the VeriSign CPS.

The *Aviareto RA Component* private key will be activated when the component is started and a password has been entered. A password meeting the requirements of section 6.4 must be used.

A Registry User must use a password meeting the requirements of section 6.4 in order to activate his private key. All Registry Users shall take all reasonable steps to protect the activation password for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.9. Method of deactivating private key

Aviareto CA private keys shall be activated as specified in the *VeriSign CPS.*

The Registry User private key will be deactivated once it has been revoked by the *Aviareto RA Operator* or an Administrator (depending on the type of Registry User), or the Registry User's certificate has expired.

6.2.10. Method of destroying private key

Aviareto CA private keys shall be destroyed as specified in the *VeriSign CPS.*

6.2.11. Cryptographic Module Rating

Please refer to the *VeriSign CPS.*

A HSM is used to protect the *Aviareto RA Component* private key.

A JKS keystore is used to protect the *Aviareto RA Operator* keystore and the subscriber keystore.

6.3. Other aspects of key pair management

6.3.1. Public key archival

All public keys are archived as specified in the *VeriSign CPS.*

6.3.2. Certificate operational periods and key pair usage periods

The operational period of each certificate ends upon its expiration or revocation. Public keys with associated expired or revoked certificates may be used for verifying signatures that were created before the certificate expired or was revoked.

6.4. Activation data

Aviareto strongly recommends the use of strong passwords to protect private keys according to the specification in the *VeriSign CPS.* Aviareto therefore recommends that passwords:

- be generated by the user;
- have at least eight characters;
- have at least one alphabetic and one numeric character;
- have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long substring of the user's profile name.

6.4.1. Activation data generation and installation

Please refer to the *VeriSign CPS for* activation data used to protect tokens containing the *Aviareto CA* private key.

6.4.2. Activation data protection

Passwords are required to access all keystores. The password should follow the recommendations in section 6.4.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

Please refer to the *VeriSign CPS* for specific computer security controls relating to the *Aviareto CA*.

6.5.2. Computer security rating

Please refer to the *VeriSign CPS* for specific computer security ratings relating to the *Aviareto CA*.

6.6. Life cycle technical controls

6.6.1. System development controls

Please refer to the *VeriSign CPS.*

6.6.2. Security management controls

Please refer to the *VeriSign CPS.*

6.6.3. Life cycle security controls

Please refer to the *VeriSign CPS.*

6.7. Network security controls

Please refer to the *VeriSign CPS.*

6.8. Time-stamping

Please refer to the *VeriSign CPS.*

7. Certificate, CRL, and OCSP Profile

7.1. Certificate profile

7.1.1. Version number(s)

All certificates issued by Aviareto will be RFC 3280 X.509 Version 3 Certificates.

7.1.2. Certificate extensions

7.1.2.1. keyUsage

The *keyUsage* extension defines the purpose (e.g., encipherment, digital signature, certificate signing) of the key contained in the certificate.

The *keyUsage* extensions of the *Aviareto Root CA* and *Aviareto Subordinate CA* certificates are both set to *keyCertSign* and *CRLsign*

The *keyUsage* extension of the Registry User certificate is set to *digitalSignature* and *nonRepudiation*.

7.1.2.2.basicConstraints

The *basicConstraints* extension identifies whether the subject of the certificate is a CA and how deep a certification path may exist through that CA.

The *basicConstraints* extension of the *Aviareto Root CA* certificate is set to *CA* and *1* (meaning that it is a CA with 1 Subordinate CA below it) and the *basicConstraints* extension of the *Aviareto Subordinate CA* certificate is set to *CA* and *0* (meaning that it is a CA with 0 subordinates CA below it).

7.1.2.3.crlDistributionPoint

The *crlDistributionPoint* extension identifies how CRL information is obtained.

The *crlDistributionPoint* extension of the *Aviareto Root CA* certificate is not set because this is a root CA. The *crlDistributionPoint* extension of the *Aviareto Subordinate CA* certificate is set to:

URI=http://onsitecrl.verisign.com/offlineca/AviaretoLtd InternationalRegistryCA/RootCA.crl

The *crlDistributionPoint* extension of the *Registry User* certificate is set to:

URI=http://onsitecrl.verisign.com/AviaretoLtdInternationalRegistryCA/Latest CRL.crl

7.1.2.4.SubjectAlternativeName

The *subjectAlternativeName* extension allows additional identities to be bound to the subject (DN) of the certificate.

The *subjectAlternativeName* extension of the *Aviareto Root CA* certificate is used by VeriSign and not configurable

The *subjectAlternativeName* extension of the *Aviareto Subordinate CA* certificate is used by VeriSign and not configurable

The *subjectAlternativeName* extension of the Registry User certificate is not configured on the Aviareto end user certificates

7.1.3. Algorithm object identifiers

Aviareto certificates are signed using this algorithm:

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }

7.1.4. Name forms

The Registry User certificate shall contain the full Distinguished Name of the certificate subject and certificate issuer.

7.1.5. Name constraints

Not Implemented

7.1.6. Certificate policy object identifier

Not applicable.

7.1.7. Usage of Policy Constraints extension

Not Implemented

7.1.8. Policy qualifiers syntax and semantics

Not Implemented

7.1.9. Processing semantics for the critical Certificate Policies extension

Critical marked certificate extensions must be treated in accordance with PKIX Part1.

7.2. CRL profile

7.2.1. Version number(s)

The CRL issued by the *Aviareto Root CA* and the *Aviareto Subordinate CA* is in accordance with RFC 3280 X.509 Version 2.

7.2.2. CRL and CRL entry extensions

Please refer to the *VeriSign CPS.*

7.3. OCSP profile

7.3.1. Version number(s)

Not Implemented

7.3.2. OCSP extensions

Not Implemented

8. Compliance audit

8.1. Frequency or circumstances of assessment

Please refer to the *VeriSign CPS.*

8.2. Identity/qualifications of assessor

Please refer to the *VeriSign CPS.*

8.3. Assessor's relationship to assessed entity

Please refer to the *VeriSign CPS.*

8.4. Topics covered by assessment

Please refer to the *VeriSign CPS.*

8.5. Actions taken as a result of deficiency

Please refer to the *VeriSign CPS.*

8.6. Communication of results

Please refer to the *VeriSign CPS.*

9. Other Business and Legal Matters

9.1. Fees

The PKI functionality provided in accordance with this CPS is one of the components of the Registry. The fee structure is as defined in the Procedures.

The fees include the provision of a Digital Certificate which is installed on the Registry User's workstation. The private key of the Digital Certificate may not be exported or copied to another workstation by the Registry User, save where permitted by the Procedures. In the event of this Digital Certificate being lost or destroyed, a new Digital Certificate will be supplied in accordance with this CPS on payment of the "Lost Certificate Fee" as set out in the fee structure.

9.2. Privacy of personal information

9.2.1. Privacy Policy

Aviareto has implemented a privacy policy. The privacy policy can be found at www.internationalregistry.aero.

9.3. Representations and warranties

9.3.1. Registry User representations and warranties

1) By accepting a Digital Certificate issued by Aviareto, until the Registry User notifies via email otherwise, the Registry User warrants to Aviareto

at the time of acceptance and throughout the operational period of the Digital Certificate that to its actual knowledge:

a) each digital signature created using the private key corresponding to the public key listed in the Digital Certificate is the digital signature of the Registry User and the Digital Certificate has been accepted and is operational (not expired, suspended or revoked) and not compromised in any way at the time the digital signature is created;

b) no unauthorised personnel have ever had access to the Registry User's private key which would be expected to result in unauthorised registrations;

c) all representations made by the Registry User to Aviareto regarding the information contained in the Digital Certificate are true;

d) all information contained in the Digital Certificate is true insofar as it is derived from information provided by the Registry User and if not derived from such information, is true to the extent that the Registry User had knowledge or notice of any such information;

e) the Registry User has promptly notified Aviareto of any material inaccuracies in such information contained in the Digital Certificate;

f) the Digital Certificate is being used exclusively for authorised and legal purposes, consistent with this CPS;

g) the Registry User is an end user subscriber and not a CA, and will not use the private key corresponding to any public key listed in the certificate for the purposes of signing any certificate (or any other format of certified public key) as a CA or otherwise;

h) all information and representations contained in the Registry User's application for a Digital Certificate and in all subsequent communications with Aviareto are accurate, true and correct in all material respects;

i) it shall take all reasonable steps to ensure that its private key is protected and so as to prevent the compromise or unauthorised use of that private key;

j) it shall notify Aviareto immediately via email to "registryofficial@aviareto.aero" upon compromise or unauthorised use of its private key;

k) it shall implement reasonable internal measures and safeguards to ensure appropriate use of its private key at all times; and

l) it shall only use the Digital Certificate for the purposes of the International Registry in accordance with the *Registry User Terms and Conditions,* the procedures and the CPS.

9.4. Disclaimers of warranties

Each Registry User acknowledges and agrees that:

1) by issuing a Digital Certificate Aviareto does not grant any rights or privileges except as set out in this CPS;

2) Aviareto shall have no liability associated in any way with the loss by a Digital Subscriber of its private key;

3) Aviareto shall have no liability associated in any way with subscriber generated keys unless they were generated fully in accordance with the guidelines set out in this CPS;

4) Aviareto shall have no liability associated with compromise of the private keys it produces, unless the keys were compromised by Aviareto;

5) Aviareto shall have no liability associated with a forged signature;

6) Aviareto shall have no liability associated with the wrongful binding of an individual's identity with an associated digital signature, where the documented policies and procedures for the identification and authentication were followed;

7) Aviareto shall have no liability for any error, corruption of data or any amendment of information transmitted, which occurs when a Digital Certificate or any other communication enters on information system, or the first information system outside the control of Aviareto, in each case to the extent set in the Convention, Protocol, Regulations, and Terms and Conditions.

8) Aviareto shall have no liability associated with lack of accessibility caused by

   (i) the public internet; or

   (ii) the systems and browser software used by the Registry User.

9.5. Limitations of Liability

The Registrar's liability under or in connection with this CPS shall be as provided in the Convention, Protocol, Regulations, Procedures, and Terms and Conditions.

9.6. Term and termination

9.6.1. Term

This CPS becomes effective upon publication on the Website. Amendments to this CPS become effective upon publication on the Aviareto web site

9.6.2. Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version.

9.6.3. Effect of termination and survival

Upon termination of this CPS, Registry Users and Registry User Entities are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.7. Individual notices and communications with participants

9.8. Amendments

This CPS can be amended by a revised version being posted on the Website.

9.9. Dispute resolution provisions

9.9.1. Disputes with Registry Users, Administrators of Registry User Entities and Aviareto

Disputes between Registry Users, Administrators of Registry User Entities and Aviareto require written notification to Registry Officials (registryofficial@aviareto.aero) as set out in the Procedues. Following written notification of a dispute the Registry Official will coordinate resolution as appropriate.

9.10. Governing law

See Terms and Conditions.

9.11. Compliance with applicable law

Each Registry User and Aviareto shall observe and abide by all laws, regulations and by laws as may apply in relation to the matters contemplated by this CPS.

9.12. Miscellaneous provisions

9.12.1. Assignment

No Registry User or Registry User Entity may assign or otherwise transfer to any other person any Digital Certificate or any aspect of the arrangements contemplated by this CPS.

9.12.2. Force Majeure

Aviareto shall not have any liability or deemed to be in default for any delays or failures in performance of any of its obligations under the CPS resulting from any event outside of its reasonable control, including but not limited to act of God, governmental act, failure of systems or telecommunications networks, war, fire, flood, explosion or civil commotion, in all cases to the extent that it is not liable therefor under Article 28 of the Convention.

9.13. Other provisions

9.13.1. NO FIDUCIARY RELATIONSHIPS

1) Aviareto is not the agent, fiduciary, trustee or other representative of any Registry User or Registry User Entity.

2) Registry Users and Registry User Entities shall have no authority to bind Aviareto, by contract or otherwise, to any obligation.