A close up of a logo

Description automatically generated A close up of a sign

Description automatically generated

IATA ONE Record

Certificate Policy (CP) for TSL Client and Server Certificates approved as authentication factor for ONE Record services

|  |  |
| --- | --- |
| **Date**: 25/2/2019 | **Version**: |
| **Status**: | **No. Of Pages**: 43 |
| **OID**: | **Classification**: |
| **File**: IATA1R - CP TSL Certificates.v1.0.docx | |
| **Published by**: <IATA Department responsible of this document> | |

This document is issued by IATA and licensed under a **Creative Commons Attribution - No Derivatives 4.0 (CC BY-ND 4.0)**.

Documentation management

Document Approval

|  |  |  |
| --- | --- | --- |
| Version | IATA Representative #1 | IATA Representative #2 |
| 1.1 | Name:  Signature: | Name:  Signature: |

Version history

|  |  |  |
| --- | --- | --- |
| Version | Date | Comments |
| 1.0 | 15/3/2020 | First version |
| 1.1 | 20/3/2020 | Changes in Introduction Section |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1 Introductions 9](#_Toc35598506)

[1.1 Overview 9](#_Toc35598507)

[1.2 Document Name and Identification 10](#_Toc35598508)

[1.3 PKI Participants 10](#_Toc35598509)

[1.3.1 Certification authorities 10](#_Toc35598510)

[1.3.2 Registration authorities 10](#_Toc35598511)

[1.3.3 Subscribers 10](#_Toc35598512)

[1.3.4 Relying parties 10](#_Toc35598513)

[1.3.5 Other participants 10](#_Toc35598514)

[1.4 Certificate Usage 11](#_Toc35598515)

[1.4.1 Appropriate Certificate Uses 11](#_Toc35598516)

[1.4.2 Prohibited certificate uses 11](#_Toc35598517)

[1.5 Policy Administration 11](#_Toc35598518)

[1.5.1 Organization administering the document 11](#_Toc35598519)

[1.5.2 Contact Person (Contact Information) 11](#_Toc35598520)

[1.5.3 Person determining CPS suitability for the policy 12](#_Toc35598521)

[1.5.4 CPS approval procedures 12](#_Toc35598522)

[1.6 Definitions and Acronyms 12](#_Toc35598523)

[2 Publication and Repository Responsibilities 13](#_Toc35598524)

[2.1 Repositories 13](#_Toc35598525)

[2.2 Publication 13](#_Toc35598526)

[2.3 Time or frequency of publication 13](#_Toc35598527)

[2.4 Access control on repositories 13](#_Toc35598528)

[3 Identification and Authentication 14](#_Toc35598529)

[3.1 Naming 14](#_Toc35598530)

[3.1.1 Types of names 14](#_Toc35598531)

[3.1.2 Need for names to be meaningful 14](#_Toc35598532)

[3.1.3 Anonymity of subscribers and pseudonyms 14](#_Toc35598533)

[3.1.4 Rules for interpreting various name forms 14](#_Toc35598534)

[3.1.5 Uniqueness of names 14](#_Toc35598535)

[3.1.6 Recognition, authentication, and role of trademarks 15](#_Toc35598536)

[3.2 Initial Identity Validation 15](#_Toc35598537)

[3.2.1 Method to prove possession of private key 15](#_Toc35598538)

[3.2.2 Authentication of organization identity 15](#_Toc35598539)

[3.2.3 Authentication of individual identity 15](#_Toc35598540)

[3.2.4 Non-verified subscriber information 15](#_Toc35598541)

[3.2.5 Validation of authority 16](#_Toc35598542)

[3.2.6 Criteria for interoperation 16](#_Toc35598543)

[3.3 Identification and Authentication for Re-key Requests 16](#_Toc35598544)

[3.3.1 Identification and authentication for routine re-key 16](#_Toc35598545)

[3.3.2 Identification and authentication for re-key after revocation 16](#_Toc35598546)

[3.4 Identification and Authentication for Revocation Requests 16](#_Toc35598547)

[4 Certificate Life-Cycle Operational Requirements 17](#_Toc35598548)

[4.1 Certificate Application 17](#_Toc35598549)

[4.1.1 Who can submit a certificate application? 17](#_Toc35598550)

[4.1.2 Enrolment process and responsibilities 17](#_Toc35598551)

[4.2 Certificate Application Processing 17](#_Toc35598552)

[4.2.1 Performing identification and authentication functions 17](#_Toc35598553)

[4.2.2 Approval or rejection of certificate applications 17](#_Toc35598554)

[4.2.3 Time to process certificate applications 17](#_Toc35598555)

[4.3 Certificate Issuance 18](#_Toc35598556)

[4.3.1 CA actions during certificate issuance 18](#_Toc35598557)

[4.3.2 Notifications to subscriber by the CA of issuance of certificate 18](#_Toc35598558)

[4.4 Certificate Acceptance 18](#_Toc35598559)

[4.4.1 Conduct constituting certificate acceptance 18](#_Toc35598560)

[4.4.2 Publication of the certificate by the CA 18](#_Toc35598561)

[4.4.3 Notification of certificate issuance by the CA to other entities 18](#_Toc35598562)

[4.5 Key Pair and Certificate Usage 18](#_Toc35598563)

[4.5.1 Subscriber private key and certificate usage 18](#_Toc35598564)

[4.5.2 Relying party public key and certificate usage 18](#_Toc35598565)

[4.6 Certificate Renewal 18](#_Toc35598566)

[4.6.1 Circumstance for certificate renewal 19](#_Toc35598567)

[4.6.2 Who may request renewal? 19](#_Toc35598568)

[4.6.3 Processing certificate renewal requests 19](#_Toc35598569)

[4.6.4 Notification of new certificate issuance to subscriber 19](#_Toc35598570)

[4.6.5 Conduct constituting acceptance of a renewal certificate 19](#_Toc35598571)

[4.6.6 Publication of the renewal certificate by the CA 19](#_Toc35598572)

[4.6.7 Notification of certificate issuance by the CA to other entities 19](#_Toc35598573)

[4.7 Certificate Re-key 19](#_Toc35598574)

[4.7.1 Circumstance for certificate re-key 19](#_Toc35598575)

[4.7.2 Who may request certification of a new public key? 19](#_Toc35598576)

[4.7.3 Processing certificate re-keying requests 19](#_Toc35598577)

[4.7.4 Notification of new certificate issuance to subscriber 19](#_Toc35598578)

[4.7.5 Conduct constituting acceptance of a re-keyed certificate 19](#_Toc35598579)

[4.7.6 Publication of the re-keyed certificate by the CA 20](#_Toc35598580)

[4.7.7 Notification of certificate issuance by the CA to other entities 20](#_Toc35598581)

[4.8 Certificate Modification 20](#_Toc35598582)

[4.8.1 Circumstance for certificate modification 20](#_Toc35598583)

[4.8.2 Who may request certificate modification? 20](#_Toc35598584)

[4.8.3 Processing certificate modification requests 20](#_Toc35598585)

[4.8.4 Notification of new certificate issuance to subscriber 20](#_Toc35598586)

[4.8.5 Conduct constituting acceptance of modified certificate 20](#_Toc35598587)

[4.8.6 Publication of the modified certificate by the CA 20](#_Toc35598588)

[4.8.7 Notification of certificate issuance by the CA to other entities 20](#_Toc35598589)

[4.9 Certificate Revocation and Suspension 20](#_Toc35598590)

[4.9.1 Circumstances for revocation 21](#_Toc35598591)

[4.9.2 Who can request revocation? 21](#_Toc35598592)

[4.9.3 Procedure for revocation request 21](#_Toc35598593)

[4.9.4 Revocation request grace period 21](#_Toc35598594)

[4.9.5 Time within which CA must process the revocation request 21](#_Toc35598595)

[4.9.6 Revocation checking requirement for relying parties 21](#_Toc35598596)

[4.9.7 CRL issuance frequency 21](#_Toc35598597)

[4.9.8 Maximum latency for CRLs 21](#_Toc35598598)

[4.9.9 On-line revocation/status checking availability 21](#_Toc35598599)

[4.9.10 On-line revocation checking requirements 21](#_Toc35598600)

[4.9.11 Other forms of revocation advertisements available 21](#_Toc35598601)

[4.9.12 Special requirements regarding key compromise 21](#_Toc35598602)

[4.9.13 Circumstances for suspension 21](#_Toc35598603)

[4.9.14 Who can request suspension? 21](#_Toc35598604)

[4.9.15 Procedure for suspension request 21](#_Toc35598605)

[4.9.16 Limits on suspension period 22](#_Toc35598606)

[4.10 Certificate Status Services 22](#_Toc35598607)

[4.10.1 Operational characteristics 22](#_Toc35598608)

[4.10.2 Service availability 22](#_Toc35598609)

[4.10.3 Optional features 22](#_Toc35598610)

[4.11 End of Subscription 22](#_Toc35598611)

[4.12 Key Escrow and Recovery 22](#_Toc35598612)

[4.12.1 Key escrow and recovery policy and practices 22](#_Toc35598613)

[4.12.2 Session key encapsulation and recovery policy and practices 22](#_Toc35598614)

[5 Management, Operational, and Physical Controls 23](#_Toc35598615)

[5.1 Physical Security Controls 23](#_Toc35598616)

[5.1.1 Site location and construction 23](#_Toc35598617)

[5.1.2 Physical access 23](#_Toc35598618)

[5.1.3 Power and air conditioning 23](#_Toc35598619)

[5.1.4 Water exposures 23](#_Toc35598620)

[5.1.5 Fire prevention and protection 23](#_Toc35598621)

[5.1.6 Media storage 23](#_Toc35598622)

[5.1.7 Waste disposal 23](#_Toc35598623)

[5.1.8 Backup 23](#_Toc35598624)

[5.2 Procedural Controls 23](#_Toc35598625)

[5.2.1 Trusted roles 23](#_Toc35598626)

[5.2.2 Number of persons required per task 23](#_Toc35598627)

[5.2.3 Identification and authentication for each role 23](#_Toc35598628)

[5.2.4 Roles requiring separation of duties 24](#_Toc35598629)

[5.3 Personnel Security Controls 24](#_Toc35598630)

[5.3.1 Qualifications, experience, and clearance requirements 24](#_Toc35598631)

[5.3.2 Background check procedures 24](#_Toc35598632)

[5.3.3 Training requirements 24](#_Toc35598633)

[5.3.4 Retraining frequency and requirements 24](#_Toc35598634)

[5.3.5 Job rotation frequency and sequence 24](#_Toc35598635)

[5.3.6 Sanctions for unauthorized actions 24](#_Toc35598636)

[5.3.7 Independent contractor requirements 24](#_Toc35598637)

[5.3.8 Documentation supplied to personnel 24](#_Toc35598638)

[5.3.9 Contract termination and assigned role change procedures 24](#_Toc35598639)

[5.4 Audit Logging Procedures 24](#_Toc35598640)

[5.4.1 Types of events recorded 24](#_Toc35598641)

[5.4.2 Frequency of processing log 24](#_Toc35598642)

[5.4.3 Retention period for audit log 25](#_Toc35598643)

[5.4.4 Protection of audit log 25](#_Toc35598644)

[5.4.5 Audit log backup procedures 25](#_Toc35598645)

[5.4.6 Audit collection system (internal vs. external) 25](#_Toc35598646)

[5.4.7 Notification to event-causing subject 25](#_Toc35598647)

[5.4.8 Vulnerability assessments 25](#_Toc35598648)

[5.5 Records Archival 25](#_Toc35598649)

[5.5.1 Types of records archived 25](#_Toc35598650)

[5.5.2 Retention period for archive 25](#_Toc35598651)

[5.5.3 Protection of archive 25](#_Toc35598652)

[5.5.4 Archive backup procedures 25](#_Toc35598653)

[5.5.5 Requirements for timestamping of records 25](#_Toc35598654)

[5.5.6 Archive collection system (internal or external) 25](#_Toc35598655)

[5.5.7 Procedures to obtain and verify archive information 25](#_Toc35598656)

[5.6 Key Changeover 26](#_Toc35598657)

[5.7 Compromise and Disaster Recovery 26](#_Toc35598658)

[5.7.1 Incident and compromise handling procedures 26](#_Toc35598659)

[5.7.2 Computing resources, software, and/or data are corrupted 26](#_Toc35598660)

[5.7.3 Entity private key compromise procedures 26](#_Toc35598661)

[5.7.4 Business continuity capabilities after a disaster 26](#_Toc35598662)

[5.8 CA or RA Termination 26](#_Toc35598663)

[6 Technical Security Controls 27](#_Toc35598664)

[6.1 Key Pair Generation and Installation 27](#_Toc35598665)

[6.1.1 Key pair generation 27](#_Toc35598666)

[6.1.2 Private key delivery to subscriber 27](#_Toc35598667)

[6.1.3 Public key delivery to certificate issuer 27](#_Toc35598668)

[6.1.4 CA public key delivery to relying parties 27](#_Toc35598669)

[6.1.5 Key sizes 27](#_Toc35598670)

[6.1.6 Public key parameters generation and quality checking 27](#_Toc35598671)

[6.1.7 Key usage purposes (as per X.509 v3 key usage field) 27](#_Toc35598672)

[6.2 Private Key Protection and Cryptographic Module Engineering Controls 27](#_Toc35598673)

[6.2.1 Cryptographic module standards and controls 28](#_Toc35598674)

[6.2.2 Private key (n out of m) multi-person control 28](#_Toc35598675)

[6.2.3 Private key escrow 28](#_Toc35598676)

[6.2.4 Private key backup 28](#_Toc35598677)

[6.2.5 Private key archival 28](#_Toc35598678)

[6.2.6 Private key transfer into or from a cryptographic module 28](#_Toc35598679)

[6.2.7 Private key storage on cryptographic module 28](#_Toc35598680)

[6.2.8 Method of activating private key 28](#_Toc35598681)

[6.2.9 Method of deactivating private key 28](#_Toc35598682)

[6.2.10 Method of destroying private key 28](#_Toc35598683)

[6.2.11 Cryptographic Module Rating 28](#_Toc35598684)

[6.3 Other Aspects of Key Pair Management 28](#_Toc35598685)

[6.3.1 Public key archival 28](#_Toc35598686)

[6.3.2 Certificate operational periods and key pair usage periods 28](#_Toc35598687)

[6.4 Activation Data 29](#_Toc35598688)

[6.4.1 Activation data generation and installation 29](#_Toc35598689)

[6.4.2 Activation data protection 29](#_Toc35598690)

[6.4.3 Other aspects of activation data 29](#_Toc35598691)

[6.5 Computer Security Controls 29](#_Toc35598692)

[6.5.1 Specific computer security technical requirements 29](#_Toc35598693)

[6.5.2 Computer security rating 29](#_Toc35598694)

[6.6 Life Cycle Security Controls 29](#_Toc35598695)

[6.6.1 System development controls 29](#_Toc35598696)

[6.6.2 Security management controls 29](#_Toc35598697)

[6.6.3 Life cycle security controls 29](#_Toc35598698)

[6.7 Network Security Controls 29](#_Toc35598699)

[6.8 Timestamping 29](#_Toc35598700)

[7 Certificate and CRL Profiles 30](#_Toc35598701)

[7.1 Certificate Profile 30](#_Toc35598702)

[7.1.1 Version number(s) 30](#_Toc35598703)

[7.1.2 Certificate extensions 30](#_Toc35598704)

[7.1.3 Algorithm object identifiers 31](#_Toc35598705)

[7.1.4 Name forms 32](#_Toc35598706)

[7.1.5 Name constraints 32](#_Toc35598707)

[7.1.6 Certificate policy object identifier 32](#_Toc35598708)

[7.1.7 Usage of Policy Constraints extension 32](#_Toc35598709)

[7.1.8 Policy qualifiers syntax and semantics 32](#_Toc35598710)

[7.1.9 Processing semantics for the critical Certificate Policies extension 32](#_Toc35598711)

[7.2 CRL Profile 32](#_Toc35598712)

[7.2.1 Version number(s) 32](#_Toc35598713)

[7.2.2 CRL Profile and CRL entry extensions 32](#_Toc35598714)

[7.3 OCSP Profile 33](#_Toc35598715)

[7.3.1 Version number(s) 33](#_Toc35598716)

[7.3.2 OCSP extensions 33](#_Toc35598717)

[8 Compliance Audit and Other Assessment 34](#_Toc35598718)

[8.1 Frequency or circumstances of assessment 34](#_Toc35598719)

[8.2 Identity/qualifications of assessor 34](#_Toc35598720)

[8.3 Assessor's relationship to assessed entity 34](#_Toc35598721)

[8.4 Topics covered by assessment 34](#_Toc35598722)

[8.5 Actions taken as a result of deficiency 34](#_Toc35598723)

[8.6 Communication of results 34](#_Toc35598724)

[9 Other Business and Legal Matters 35](#_Toc35598725)

[9.1 Fees 35](#_Toc35598726)

[9.1.1 Certificate issuance or renewal fees 35](#_Toc35598727)

[9.1.2 Certificate access fees 35](#_Toc35598728)

[9.1.3 Revocation or status information access fees 35](#_Toc35598729)

[9.1.4 Fees for other services 35](#_Toc35598730)

[9.1.5 Refund policy 35](#_Toc35598731)

[9.2 Financial Responsibility 35](#_Toc35598732)

[9.2.1 Insurance coverage 35](#_Toc35598733)

[9.2.2 Other assets 35](#_Toc35598734)

[9.2.3 Insurance or warranty coverage for end-entities 35](#_Toc35598735)

[9.3 Confidentiality of Business Information 35](#_Toc35598736)

[9.3.1 Scope of confidential information 35](#_Toc35598737)

[9.3.2 Information not within the scope of confidential information 35](#_Toc35598738)

[9.3.3 Responsibility to protect confidential information 36](#_Toc35598739)

[9.4 Privacy of Personal Information 36](#_Toc35598740)

[9.4.1 Privacy plan 36](#_Toc35598741)

[9.4.2 Information treated as private 36](#_Toc35598742)

[9.4.3 Information not deemed private 36](#_Toc35598743)

[9.4.4 Responsibility to protect private information 36](#_Toc35598744)

[9.4.5 Notice and consent to use private information 36](#_Toc35598745)

[9.4.6 Disclosure pursuant to judicial or administrative process 36](#_Toc35598746)

[9.4.7 Other information disclosure circumstances 36](#_Toc35598747)

[9.5 Intellectual Property Rights 36](#_Toc35598748)

[9.6 Representations and Warranties 36](#_Toc35598749)

[9.6.1 CA representations and warranties 36](#_Toc35598750)

[9.6.2 RA representations and warranties 36](#_Toc35598751)

[9.6.3 Subscriber representations and warranties 36](#_Toc35598752)

[9.6.4 Relying party representations and warranties 37](#_Toc35598753)

[9.6.5 Representations and warranties of other participants 37](#_Toc35598754)

[9.7 Disclaimers of Warranties 37](#_Toc35598755)

[9.8 Limitations of Liability 37](#_Toc35598756)

[9.9 Indemnities 37](#_Toc35598757)

[9.10 Term and Termination 37](#_Toc35598758)

[9.10.1 Term 37](#_Toc35598759)

[9.10.2 Termination 37](#_Toc35598760)

[9.10.3 Effect of termination and survival 37](#_Toc35598761)

[9.11 Individual notices and communications with participants 37](#_Toc35598762)

[9.12 Amendments 37](#_Toc35598763)

[9.12.1 Procedure for amendment 37](#_Toc35598764)

[9.12.2 Notification mechanism and period 37](#_Toc35598765)

[9.12.3 Circumstances under which OID must be changed 37](#_Toc35598766)

[9.13 Dispute Resolution Procedures 38](#_Toc35598767)

[9.14 Governing Law 38](#_Toc35598768)

[9.15 Compliance with Applicable Law 38](#_Toc35598769)

[9.16 Miscellaneous Provisions 38](#_Toc35598770)

[9.16.1 Entire agreement 38](#_Toc35598771)

[9.16.2 Assignment 38](#_Toc35598772)

[9.16.3 Severability 38](#_Toc35598773)

[9.16.4 Enforcement (attorneys' fees and waiver of rights) 38](#_Toc35598774)

[9.16.5 Force Majeure 38](#_Toc35598775)

[9.17 Other Provisions 38](#_Toc35598776)

[10 Annex A: Glossary 39](#_Toc35598777)

# Introductions

## Overview

**About IATA**: The International Air Transport Association (IATA) is the trade association for the world’s airlines, representing some 290 airlines or 82% of total air traffic. IATA’s mission is to represent, lead, and serve the airline industry and it supports many areas of aviation activity and helps formulate industry policy on critical aviation issues. For over 70 years, IATA has developed global commercial standards upon which the air transport industry is built. Its aim is to assist airlines by simplifying processes and increasing passenger convenience while reducing costs and improving efficiency.

ONE Record is a standard for data sharing and creates a single record view of a shipment. This standard defines a common data model for the data that is shared via standardized and secured web API. The vision for ONE Record is an end-to-end digital logistics and transport supply chain where data is easily and transparently exchanged in a digital ecosystem of air cargo stakeholders, communities and data platforms. ONE Record uses an industry-wide and federated trust network to manage identification and authentication of data sharing systems and ensures data privacy and confidentiality for all parties.

This Certification Policy (CP) document published by IATA describe the stipulations to be implemented by any Certification Authority, adhered to the ONE Record Project, in order to issue and manage certificates of approved to authenticate and protect entities serving or consuming ONE Record services.

This document is developed per the recommendations found in the document **RFC3647** issued by *The Internet Engineering Task Force (IETF)* in 2003, which has been adopted as a worldwide-recognized standard framework to document the Certifications Practice Statement and related Certificate Policies disclosed by a Certification Services Provider.

The purpose of the CP documents is to disclose the Policies to be adopted in the **1RPKI** for the issuance of digital certificates. It is organized in the following sections:

1. Introductions – This section. Introduces the **1RPKI** and this document.
2. Publication and Repositories Responsibilities – Describes the publication policies for the certificates affected by this document, and the publication of this document itself.
3. Identification and Authentication – Discloses the rules for subscriber naming and required authentication policies.
4. Certificate Life-Cycle Operational Requirements – This section describes the different phases in the Lifecycle of certificates and their requirements.
5. Management, Operational and Physical Controls – Describes the controls enforced in the **1RPKI** to provide adequate trust levels in the certificates issued under the Trust Model.
6. Technical Security Controls – Discloses the security controls adopted in the **1RPKI**.
7. Certificate and CRL Profiles – Describes the technical details of the different certificate types issued under the **1RPKI**.
8. Compliance Audit and other Assessment – Discloses the audit policies followed in the **1RPKI** to ensure that the participant fulfils the security and quality requirements.
9. Other Business and Legal Matters – This section exposes the commercial, legal and contractual aspects involved in the usage of certificates issued in the **1RPKI**.

## Document Name and Identification

|  |  |
| --- | --- |
| **Name** | 1RPKI Certificate Policy for TLS Certificates |
| **Version** | 1.0 |
| **OID** | DOCUMENT\_ID |
| **Issuance date** | <PUBLISHING\_DATE> |
| **Location** | This document can be found at /<URL> |

## PKI Participants

### Certification authorities

The current full list of Certification Authorities that have been authorized by IATA to operate under the **1RPKI** and implement this particular CP is disclosed in **https://www.iata.org/<URL>**.

### Registration authorities

*As stipulated in the CPS published by the Issuing CA.*

### Subscribers

In the **1RPKI** two different end-user roles are defined. Depending on the status of the certificate request, these roles are named “Applicant” and “Subscriber”.

An *applicant* is a physical person that requests a certificate for his own behalf or on behalf of a third party. The applicant needs to accredit his identity and ability to request a certificate. In the case of an applicant acting on behalf of a third party or legal person, he will be requested to accredit the empowerment for such representation, as required by law.

A *subscriber* is the physical or legal person whose identity is linked to the electronic signature creation data, or private key, and included in a digital certificate. In general, a subscriber is considered the “owner” of a certificate. The subscriber of a certificate is responsible for the custody of his private key and not communicating this data in any way to any other person.

Subscribers for certificates issued under this CP are, in particular, natural and legal persons requiring to protect their internet and communication servers implementing the ONE Record Protocol, by means of client/server authentication and encryption.

### Relying parties

All persons and entities that trust the certificates issued by certification authorities operating under the **1RPKI** Trust Model are considered to be “relying parties” (or trusted third parties). These relying parties do not necessarily need to be a subscriber of an **1RPKI** certificate but are requested to accept the “Relying Party agreement “, as disclosed by the Issuing CA in its CPS.

### Other participants

*As stipulated in the CPS published by the Issuing CA.*

## Certificate Usage

### Appropriate Certificate Uses

|  |  |  |
| --- | --- | --- |
| CP Identifier | Description | Permitted uses |
| 1R Server Certificate | High assurance SSL/TLS certificate issued to pre-approved participants in the ONE Record Project to act as a Server Application.  The control on the Internet Domain is validated. Compliant with CA/Browser Forum Baseline Requirements. | Digital Signature, Encryption, **Server Authentication** |
| 1R Client Certificate | High assurance SSL/TLS certificate issued to pre-approved participants in the ONE Record Project to act as a Client Application.  The control on the any identity attribute included in the certificate is performed as described in this document. | Digital Signature, Encryption, **Client Authentication** |

### Prohibited certificate uses

In general, any usage that is not explicitly stated in section 1.4.1 of this document, is considered to be prohibited.

## Policy Administration

### Organization administering the document

This document is administered by the **1RPKI Policy Approval Authority** (referred from now as **PAA**).

The **PAA** has a series of distinct functions but does not operate as a separate legal Entity. It is managed and organized in accordance with a process that draws on expertise within IATA. The **PAA** has been established to develop, review and/or approve the practices, policies and procedures for the entire Trust Model, subject to guidelines established by the members and advisors of the IATA ONE Record project.

### Contact Person (Contact Information)

|  |  |
| --- | --- |
| **Name** | IATA -ONE Record Policy Approval Authority |
| **email address** | <EMAIL> |
| **Address** | <POSTAL ADDRESS> CH-1215 Geneva 15 (Switzerland) |

### Person determining CPS suitability for the policy

The competent entity which determines the compliance and suitability of all CPS and the different supported CPs on behalf of the entire Trust Model is the **1RPKI PAA**.

### CPS approval procedures

The **1RPKI PAA** defines and executes the procedures related to the approval of the CPS and CP and its subsequent amendments. Amendments will produce a new version of the document that will be published in the **1RPKI** Policy Repository (specified in section 2.1 of this document).

The approval of major changes of documents related to the PKI, and specially for the CPS and CP, require a meeting of the PAA and the issuance of an approval memo signed by at least two members of the PAA. Minor versions only require the participation of a single member of the PAA in order to approve the publication of a new version.

It’s required to issue new CP versions at least once a year. In the case of versioning conflict, the latest version that prevails is always the document published in the Policy Repository.

## Definitions and Acronyms

Definitions and Acronyms are included in Annex A (Glossary).

# Publication and Repository Responsibilities

This section contains the provisions regarding the publication of policies, certificates and other public information needed for the participants to interoperate with the **1RPKI**, in what respects in particular to the certificates issued to Persons. The general stipulations will be published in the appropriate CPS.

## Repositories

The main repositories of the **1RPKI** are:

* Policies repository for disclosure of CP, CPS and related information. This repository is a set of web pages and services available at the URL /<URL>
* Certificate and Certificate Revocation information repositories: *As stipulated in the CPS published by the Issuing CA.*

## Publication

*As stipulated in the CPS published by the Issuing CA.*

## Time or frequency of publication

The CPS and CP documents will be published every time they are modified, with a minimum review period of one year.

A certificate issued by any CA under the **1RPKI** will be published immediately after its issuance.

In the case of revocation of a certificate, the appropriate CA will include this revocation information in the Certificate Revocation Lists (CRL) according to section 4.9.7 (CRL issuance frequency).

## Access control on repositories

*As stipulated in the CPS published by the Issuing CA.*

# Identification and Authentication

The **1RPKI** mandates the fulfilment of a set of required minimum controls that ensure the authenticity of the data included in certificates. These controls are enforced during the full lifecycle of certificates, certificate requests, and related documents. Non-validated attributes are disallowed by this CP document.

**This document reflects the common practices to be implemented by an Issuing CA authorized to issue Client and/or Server TLS Certificates used for the ONE Record project.**

**If this CP allows multiple practices for a particular section, it must be understood that this CP will stipulate all the allowed practices and that the CPS disclosed by the Issuing CA can particularize which practices are implemented and the relevant details on the process.**

## Naming

This section describes the elements regarding naming and identifying the subscribers of **1RPKI** certificates.

### Types of names

**IATA defines the concept of “ONE Record ID” as a Uniform Resource Locator (URL) that points to a ONE Record resource. A Certificate Subscriber will be approved by IATA to use one or more “ONE Record IDs”.**

**The format of the ONE Record ID is expressed as: https://<DNS-NAME>/<COMPANY-ID>**

**Where:**

* <DNS-NAME>: An internet-reachable FQDN where the service can be located
* <COMPANY-ID>: A unique identifier assigned by IATA to the ONE Record participants

All subscriber certificates will include a Distinguished Name (DN) according to the X.501 Standard. This DN is composed only of a Common Name (CN), which includes a unique identification of the subscriber as described in section 3.1.4.2, and extracted of the Main ONE Record ID of the Subscriber. The certificates must include also additional “Subject Alternative Names” containing additional identity attributes associated to the list of ONE Record IDs .

### Need for names to be meaningful

All Names must be meaningful, and the identification the attributes associated to the subscriber must be in a human readable form.

### Anonymity of subscribers and pseudonyms

This CPdoesn’t allow anonymity or pseudonyms in the TLS certificates.

### Rules for interpreting various name forms

The rules used in the **1RPKI** to interpret the distinguished names of certificates issued under its Trust Model are defined by the ISO/IEC 9595 (X.500) Distinguished Name (DN) standard.

### Uniqueness of names

The uniqueness of names for TLS Certificates must be assured by *requiring a combination of domain names, organization name combined/associated with a unique serial alphanumeric string.*

### Recognition, authentication, and role of trademarks

*As stipulated in the CPS published by the Issuing CA.*

## Initial Identity Validation

Issuing CAs implementing this CP must perform the identity validation as stipulated in the following sections.

### Method to prove possession of private key

If the key pair is generated by the End Entity (applicant or future subscriber), then a demonstration of the possession of the private key associated to the public key is requested. Accepted means are the generation of a Certificate Signing Request (CSR) linked to the private key, or equivalent methods implemented by the Issuing CA.

### Authentication of organization identity

The authentication of organization identity for TLS certificates will follow the following rules. **The Issuing CA must detail in its CPS which of the methods are used and how are implemented.**

|  |  |
| --- | --- |
| CP Identifier | Validation Policy |
| 1R Server Certificate | The Subscribers for these certificates must be pre-approved by IATA and given some authentication code that can be used by the CA to ensure that the subscriber is entitled to request a Server Certificate.  The Issuing CA can only include in the certificate internet domains extracted of the list of “ONE Record ID” pre-approved by IATA for the subscriber.  The Issuing CA must validate the Applicant’s right to use or control each domain name that will be listed in the Subject Alternative Name field of a Certificate by using at least one of the procedures listed in section 3.2.2.4 of the Baseline Requirements issued by the CAB/Forum. |
| 1R Client Certificate | The Subscribers for these certificates must be pre-approved by IATA and given some authentication code that can be used by the CA to ensure that the subscriber is entitled to request a Client Certificate.  The Issuing CA must only include in the certificate ONE Record IDs that have been pre-approved by IATA. |

### Authentication of individual identity

The CA must ensure that the Subscriber Account used to request the certificate has been approved by IATA to act in representation of the ONE Record participant*.*

### Non-verified subscriber information

**IATA** doesn’t allow to include non-verified identity-related information in any certificate issued by a certification authority operating in the ONE Record Project.

### Validation of authority

The validation of authority for TLS certificates requires that the Subscriber Account used to request the certificate has been approved by IATA.. **The Issuing CA must detail in its CPS which of the methods are used and how are implemented.**

### Criteria for interoperation

*As stipulated in the CPS published by the Issuing CA.*

## Identification and Authentication for Re-key Requests

This section addresses the following elements for the identification and authentication procedures for re-key for each subject type (CA, RA, subscriber, and other participants). Unless otherwise specified, it can considered as equivalent the activities linked to “re-key” (new certificate for an existing subscriber, using a new key pair) and “renewal” (new certificate for an existing subscriber, using the same key pair).

### Identification and authentication for routine re-key

The certificate subscriber can request a routine re-key by authenticating himself with one of these methods:

* Username & Password
* A valid digital certificate linked to the user account

The information of the subscriber must be revalidated periodically, in particular for TLS Certificates the re-verification is required as defined by the CAB/Forum:

* 1R Server Certificates, the CA must check before each issuance that the requested list of FQDN extracted from the list ONE Record IDs is still approved by IATA, and check at least every two years that the subscriber has control on the associated internet domains
* 1R Client, the CA must check before each issuance that the requested list of ONE Record IDs is still approved by IATA

### Identification and authentication for re-key after revocation

The **1RPKI** does not support re-key of certificates after revocation. The subscriber must apply for a new digital certificate by using the same procedures as for its issuance.

## Identification and Authentication for Revocation Requests

The Identification Policy for revocation requests is the same as stipulated for routine re-keys.

# Certificate Life-Cycle Operational Requirements

The stipulations included in this section are generally disclosed in the CPS published by the Issuing CA, unless otherwise specified in the following sub-sections.

## Certificate Application

*As stipulated in the CPS published by the Issuing CA.*

### Who can submit a certificate application?

A certificate application can be submitted by the subject of the certificate or by an authorized representative of the subject, as approved by IATA.

### Enrolment process and responsibilities

The Issuer CA is responsible for ensuring that the identity of each Certificate Applicant is verified in accordance with this CP and the applicable CPS prior to the issuance of a Certificate. Applicants are responsible for submitting sufficient information and documentation to the RA to perform the required verification of identity prior to issuing a Certificate.

## Certificate Application Processing

This section describes the procedures for processing certificate applications in the **1RPKI** Trust Model.

### Performing identification and authentication functions

The identification and authentication functions can be delegated by the Issuing CA to the Registration Authorities operating under the **1RPKI**.

The steps to be executed by the Issuing CA or RA are as follows:

* As a first step, the Issuing CA or RA will perform the verifications stipulated in section 3.2.
* As a second step, the CA must check the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, according to the procedure in RFC 6844. **The Issuing CA must specify in its CPS the domains that must appear in the CAA records.**
* As a third step, the Issuing CA must check the certificate details against a list of previously revoked Certificates and rejected certificate requests to identify suspicious certificate requests.

The Issuing CA can only issue a certificate after having successfully completed the above steps.

### Approval or rejection of certificate applications

An approval of a certificate application derives from the execution of the certificate issuance procedures, as defined in the section 4.3 of this Certificate Policy and the appropriate CPS.

A rejection of a certificate application results in a notification being sent to the applicant by appropriate means and is registered for further reference.

### Time to process certificate applications

There is no time limit stipulated to complete the processing of an application.

## Certificate Issuance

An approved certificate request will be processed by the authorized responsible.

### CA actions during certificate issuance

*As stipulated in the CPS published by the Issuing CA.*

### Notifications to subscriber by the CA of issuance of certificate

*As stipulated in the CPS published by the Issuing CA.*

## Certificate Acceptance

*As stipulated in the CPS published by the Issuing CA.*

### Conduct constituting certificate acceptance

*As stipulated in the CPS published by the Issuing CA.*

### Publication of the certificate by the CA

The CAs operating under the **1RPKI** publish all issued certificates as specified in section 2 of this document.

### Notification of certificate issuance by the CA to other entities

*As stipulated in the CPS published by the Issuing CA.*

## Key Pair and Certificate Usage

The certificates issued by the **1RPKI** are used to provide authenticity, integrity, confidentiality and/or non-repudiation in electronic transactions and other computerized functions.

### Subscriber private key and certificate usage

Any party using these certificates shall use software that is compliant with X.509 and applicable IETF PKIX standards. The Issuer CA can specify restrictions on the use of a Certificate through certificate extensions and shall specify the mechanism(s) to determine certificate validity (CRLs and OCSP).

Relying Parties must process and comply with this information in accordance with their obligations as per the Relaying Party Agreement published by the Issuing CA.

### Relying party public key and certificate usage

*As stipulated in the CPS published by the Issuing CA.*

## Certificate Renewal

Certificate Renewal is understood as the issuance of a new certificate to a subscriber who maintains the key pair generated for the original certificate.

### Circumstance for certificate renewal

For TLS Certificates it is allowed the certificate renewal for the purpose of extending the validity period and always considering the requirements for re-verification periods stipulated in section 3.3 of this CP.

### Who may request renewal?

The certificate renewal can be requested by the same entities allowed to request the first issuance of the certificate.

### Processing certificate renewal requests

Certificate renewal requests are processed according to the same rules than the initial issuance*.*

### Notification of new certificate issuance to subscriber

*As stipulated in the CPS published by the Issuing CA.*

### Conduct constituting acceptance of a renewal certificate

*As stipulated in the CPS published by the Issuing CA.*

### Publication of the renewal certificate by the CA

The CAs operating under the **1RPKI** publish all issued certificates as specified in section 2 of this document.

### Notification of certificate issuance by the CA to other entities

*As stipulated in the CPS published by the Issuing CA.*

## Certificate Re-key

Certificate Re-Key is understood as the issuance of a new certificate to a subscriber that also generates a new key pair. This process is supported for all certificate types.

### Circumstance for certificate re-key

Any certificate that is not revoked can be re-keyed.

### Who may request certification of a new public key?

The certificate renewal can be requested by the same entities allowed to request the first issuance of the certificate.

### Processing certificate re-keying requests

Certificate re-key requests are processed according to the same rules than the initial issuance*.*

### Notification of new certificate issuance to subscriber

*As stipulated in the CPS published by the Issuing CA.*

### Conduct constituting acceptance of a re-keyed certificate

*As stipulated in the CPS published by the Issuing CA.*

### Publication of the re-keyed certificate by the CA

The CAs operating under the **1RPKI** publish all issued certificates as specified in section 2 of this document.

### Notification of certificate issuance by the CA to other entities

*As stipulated in the CPS published by the Issuing CA.*

## Certificate Modification

The **1RPKI** does not allow the modification of certificates during their validity period. If the information contained in a certificate ceases to be valid, or the circumstances of the subscriber change in such a manner that the conditions expressed in the CPS or the CP are not met, then the only accepted procedure is the revocation and reissuance of a new certificate.

### Circumstance for certificate modification

Does not apply.

### Who may request certificate modification?

Does not apply.

### Processing certificate modification requests

Does not apply.

### Notification of new certificate issuance to subscriber

Does not apply.

### Conduct constituting acceptance of modified certificate

Does not apply.

### Publication of the modified certificate by the CA

Does not apply.

### Notification of certificate issuance by the CA to other entities

Does not apply.

## Certificate Revocation and Suspension

All Certification Authorities operating under the **1RPKI** ensure, by establishing the necessary means, that a certificate that compromises the Trust Model for any reason is prevented from being used by either revoking or suspending that certificate.

Suspension of certificates is only supported for 1R Client Certificates, and explicitly disallowed for Server certificates, according to the CA/Browser Forum requirements, and therefore is disallowed for any certificate existing under a Root which is approved to issue publicly trusted TLS Server certificates.

The stipulations for this section must be disclosed in the CPS, and therefore the reader must refer to that document for more information.

### Circumstances for revocation

*As stipulated in the CPS published by the Issuing CA.*

### Who can request revocation?

*As stipulated in the CPS published by the Issuing CA.*

### Procedure for revocation request

*As stipulated in the CPS published by the Issuing CA.*

### Revocation request grace period

*As stipulated in the CPS published by the Issuing CA.*

### Time within which CA must process the revocation request

*As stipulated in the CPS published by the Issuing CA.*

### Revocation checking requirement for relying parties

*As stipulated in the CPS published by the Issuing CA.*

### CRL issuance frequency

*As stipulated in the CPS published by the Issuing CA.*

### Maximum latency for CRLs

*As stipulated in the CPS published by the Issuing CA.*

### On-line revocation/status checking availability

*As stipulated in the CPS published by the Issuing CA.*

### On-line revocation checking requirements

*As stipulated in the CPS published by the Issuing CA.*

### Other forms of revocation advertisements available

No stipulations.

### Special requirements regarding key compromise

*As stipulated in the CPS published by the Issuing CA.*

### Circumstances for suspension

*Suspension is not permitted for TLS Certificates.*

### Who can request suspension?

*Does not apply.*

### Procedure for suspension request

*Does not apply.*

### Limits on suspension period

*Does not apply.*

## Certificate Status Services

**For TLS Certificates, the Issuing CA must provide certificate status validation services, by means of Certificate Revocation Lists and OCSP responder. The details of such services must be detailed in the CPS published by the Issuing CA.**

### Operational characteristics

*As stipulated in the CPS published by the Issuing CA.*

### Service availability

*As stipulated in the CPS published by the Issuing CA.*

### Optional features

No stipulation.

## End of Subscription

*As stipulated in the CPS published by the Issuing CA.*

## Key Escrow and Recovery

Key escrow is not permitted for TLS Server Certificates.

### Key escrow and recovery policy and practices

*Does not apply.*

### Session key encapsulation and recovery policy and practices

*Does not apply.*

# Management, Operational, and Physical Controls

*As stipulated in the CPS published by the Issuing CA.*

## Physical Security Controls

*As stipulated in the CPS published by the Issuing CA.*

### Site location and construction

*As stipulated in the CPS published by the Issuing CA.*

### Physical access

*As stipulated in the CPS published by the Issuing CA.*

### Power and air conditioning

*As stipulated in the CPS published by the Issuing CA.*

### Water exposures

*As stipulated in the CPS published by the Issuing CA.*

### Fire prevention and protection

*As stipulated in the CPS published by the Issuing CA.*

### Media storage

*As stipulated in the CPS published by the Issuing CA.*

### Waste disposal

*As stipulated in the CPS published by the Issuing CA.*

### Backup

*As stipulated in the CPS published by the Issuing CA.*

## Procedural Controls

*As stipulated in the CPS published by the Issuing CA.*

### Trusted roles

*As stipulated in the CPS published by the Issuing CA.*

### Number of persons required per task

*As stipulated in the CPS published by the Issuing CA.*

### Identification and authentication for each role

*As stipulated in the CPS published by the Issuing CA.*

### Roles requiring separation of duties

*As stipulated in the CPS published by the Issuing CA.*

## Personnel Security Controls

*As stipulated in the CPS published by the Issuing CA.*

### Qualifications, experience, and clearance requirements

*As stipulated in the CPS published by the Issuing CA.*

### Background check procedures

*As stipulated in the CPS published by the Issuing CA.*

### Training requirements

*As stipulated in the CPS published by the Issuing CA.*

### Retraining frequency and requirements

*As stipulated in the CPS published by the Issuing CA.*

### Job rotation frequency and sequence

*As stipulated in the CPS published by the Issuing CA.*

### Sanctions for unauthorized actions

*As stipulated in the CPS published by the Issuing CA.*

### Independent contractor requirements

*As stipulated in the CPS published by the Issuing CA.*

### Documentation supplied to personnel

*As stipulated in the CPS published by the Issuing CA.*

### Contract termination and assigned role change procedures

*As stipulated in the CPS published by the Issuing CA.*

## Audit Logging Procedures

*As stipulated in the CPS published by the Issuing CA.*

### Types of events recorded

*As stipulated in the CPS published by the Issuing CA.*

### Frequency of processing log

*As stipulated in the CPS published by the Issuing CA.*

### Retention period for audit log

*As stipulated in the CPS published by the Issuing CA.*

### Protection of audit log

*As stipulated in the CPS published by the Issuing CA.*

### Audit log backup procedures

*As stipulated in the CPS published by the Issuing CA.*

### Audit collection system (internal vs. external)

*As stipulated in the CPS published by the Issuing CA.*

### Notification to event-causing subject

*As stipulated in the CPS published by the Issuing CA.*

### Vulnerability assessments

*As stipulated in the CPS published by the Issuing CA.*

## Records Archival

*As stipulated in the CPS published by the Issuing CA.*

### Types of records archived

*As stipulated in the CPS published by the Issuing CA.*

### Retention period for archive

*As stipulated in the CPS published by the Issuing CA.*

### Protection of archive

*As stipulated in the CPS published by the Issuing CA.*

### Archive backup procedures

*As stipulated in the CPS published by the Issuing CA.*

### Requirements for timestamping of records

*As stipulated in the CPS published by the Issuing CA.*

### Archive collection system (internal or external)

*As stipulated in the CPS published by the Issuing CA.*

### Procedures to obtain and verify archive information

*As stipulated in the CPS published by the Issuing CA.*

## Key Changeover

*As stipulated in the CPS published by the Issuing CA.*

## Compromise and Disaster Recovery

*As stipulated in the CPS published by the Issuing CA.*

### Incident and compromise handling procedures

*As stipulated in the CPS published by the Issuing CA.*

### Computing resources, software, and/or data are corrupted

*As stipulated in the CPS published by the Issuing CA.*

### Entity private key compromise procedures

*As stipulated in the CPS published by the Issuing CA.*

### Business continuity capabilities after a disaster

*As stipulated in the CPS published by the Issuing CA.*

## CA or RA Termination

*As stipulated in the CPS published by the Issuing CA.*

# Technical Security Controls

*Most of the stipulations of this section will refer to the CPS published by the Issuing CA. In the following sections only particular policies for TLS Certificates are stipulated, when appropriate.*

## Key Pair Generation and Installation

Under the **1RPKI**, Key Pairs are generated under the necessary securitylevels and always occurring in secure physical facilities and under the adequate personnel control.

### Key pair generation

Key Pairs for TLS Certificates can be generated by software components.

Subscribers who generate their own keys shall use a FIPS‐approved method and either a validated hardware or validated software cryptographic module, depending on the level of assurance desired.

### Private key delivery to subscriber

*As stipulated in the CPS published by the Issuing CA.*

### Public key delivery to certificate issuer

*As stipulated in the CPS published by the Issuing CA.*

### CA public key delivery to relying parties

*As stipulated in the CPS published by the Issuing CA.*

### Key sizes

The **1RPKI** enforces the use of minimum length 2048-bit RSA and ECC NIST P-256, P-384 for key pairs at all levels of the hierarchy.

The only Hashing algorithm allowed is SHA-2, with different supported variants depending on the hierarchy to which the end-entity certificate belongs, as described in 1.3.1.

### Public key parameters generation and quality checking

The algorithm used in the **1RPKI** for key generation is RSA or ECC.

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

TLS Certificates assert key usages based on the intended application of the Key Pair. In particular, Certificates to be used for digital signatures (including authentication) set the digitalSignature and keyEncipherment bits.

## Private Key Protection and Cryptographic Module Engineering Controls

The Issuing CAmust establish controls to ensure that the risks derived from a private key compromise are managed and kept under reasonable levels.

### Cryptographic module standards and controls

Requirements for End-User cryptographic devices (if any) can vary in terms of the expected assurance level, as indicated in section 6.1.1.

### Private key (n out of m) multi-person control

*As stipulated in the CPS published by the Issuing CA.*

### Private key escrow

*As stipulated in section 4.12 of this CP and in the CPS published by the Issuing CA.*

### Private key backup

*Backup for TLS Server Certificates is considered equivalent of escrow and not permitted, as stipulated in section 4.12 of this CP and in the CPS published by the Issuing CA.*

### Private key archival

*The CA shall not provide key archival services.*

### Private key transfer into or from a cryptographic module

No stipulation

### Private key storage on cryptographic module

No stipulation additional to the requirements expressed in section 6.1.

### Method of activating private key

*As stipulated in the CPS published by the Issuing CA.*

### Method of deactivating private key

*As stipulated in the CPS published by the Issuing CA.*

### Method of destroying private key

*As stipulated in the CPS published by the Issuing CA.*

### Cryptographic Module Rating

No stipulation additional to section 6.2.1.

## Other Aspects of Key Pair Management

This section includes additional stipulations regarding key pair management.

### Public key archival

*As stipulated in the CPS published by the Issuing CA.*

### Certificate operational periods and key pair usage periods

For TLS Certificates, the Certificate operational period is equivalent to the key pair usage period and limited to ONE YEAR.

## Activation Data

*As stipulated in the CPS published by the Issuing CA.*

### Activation data generation and installation

*As stipulated in the CPS published by the Issuing CA.*

### Activation data protection

*As stipulated in the CPS published by the Issuing CA.*

### Other aspects of activation data

No stipulation.

## Computer Security Controls

*As stipulated in the CPS published by the Issuing CA.*

### Specific computer security technical requirements

*As stipulated in the CPS published by the Issuing CA.*

### Computer security rating

*As stipulated in the CPS published by the Issuing CA.*

## Life Cycle Security Controls

*As stipulated in the CPS published by the Issuing CA.*

### System development controls

*As stipulated in the CPS published by the Issuing CA.*

### Security management controls

*As stipulated in the CPS published by the Issuing CA.*

### Life cycle security controls

*As stipulated in the CPS published by the Issuing CA.*

## Network Security Controls

*As stipulated in the CPS published by the Issuing CA.*

## Timestamping

*As stipulated in the CPS published by the Issuing CA.*

# Certificate and CRL Profiles

All certificates issued under the **1RPKI** must compliant to:

* ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997
* RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 (“RFC 5280”)
* Baseline Requirements for TLS Server Certificates, issued by the CA/Browser Forum

## Certificate Profile

This section refers to the certificate profiles of TLS Client and Server Certificates to be used for services publishing or consuming ONE Record Services.

### Version number(s)

All certificates in the **1RPKI** conform to X.509 Version 3.

### Certificate extensions

The different extension profiles for TLS Certificates are listed below.

#### ONE Record Server Certificate

|  |  |  |
| --- | --- | --- |
| **Authority Key Identifier** | Extension marked non-critical. | |
| **Key Identifier** | <KeyID> | |
| **Subject Key Identifier** | Extension marked non-critical | |
| **Key Identifier** | The Subject Key Identifier of the Subject of this certificate. | |
| **CRL Distribution Point** | Extension marked non-critical. | |
| **Full name** | [1]CRL Distribution Point  Distribution Point Name:  Full Name:  URL=<URL-TO-CRL> | |
| **Policy Qualifier** | See section Policy Qualifiers | |
| **Authority Information Access** | Extension marked non-critical. | |
| **Extensions** | [1]Authority Info Access  Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)  Alternative Name:  URL=<URL-TO-ISSUER-CERT>  [2]Authority Info Access  Access Method=OCSP Responder URL (1.3.6.1.5.5.7.48.1)  Alternative Name:  URL=<URL-TO-OCSP-RESPONDER> | |
| **Key Usage** | Extension marked critical. Value: Digital Signature, Key Encipherment | |
| **Extended Key Usage** | Client Authentication, Server Authentication | |
| **SubjectAltName (SAN)** | <List of SAN:DNS[[1]](#footnote-1)> (at least one) |  |
| **SubjectName** | (optional) If present, must be equal to one of the SAN |  |

#### ONE Record Client Certificate

|  |  |  |
| --- | --- | --- |
| **Authority Key Identifier** | Extension marked non-critical. | |
| **Key Identifier** | <KeyID> | |
| **Subject Key Identifier** | Extension marked non-critical | |
| **Key Identifier** | The Subject Key Identifier of the Subject of this certificate. | |
| **CRL Distribution Point** | Extension marked non-critical. | |
| **Full name** | [1]CRL Distribution Point  Distribution Point Name:  Full Name:  URL=<URL-TO-CRL> | |
| **Policy Qualifier** | See section Policy Qualifiers | |
| **Authority Information Access** | Extension marked non-critical. | |
| **Extensions** | [1]Authority Info Access  Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)  Alternative Name:  URL=<URL-TO-ISSUER-CERT>  [2]Authority Info Access  Access Method=OCSP Responder URL (1.3.6.1.5.5.7.48.1)  Alternative Name:  URL=<URL-TO-OCSP-RESPONDER> | |
| **Key Usage** | Extension marked critical. | |
| **Allowed Key Usages** | Digital Signature, Key Encipherment | |
| **Allowed Enhanced Key Usages** | Client Authentication (1.3.6.1.5.5.7.3.2) | |
| **SubjectAltName** | <List of SAN:URI[[2]](#footnote-2)> (at least one) |  |
| **SubjectName** | Must be the “CompanyID” extracted of the Main ONE Record ID, as approved by IATA |  |

### Algorithm object identifiers

The allowed Algorithm object identifiers are:

* **sha256withRSAEncryption**:  
   OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
* **ecdsa‐with‐SHA256**   
   OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(10045) pkcs(4) pkcs-1(3) 2}
* **ecdsa‐with‐SHA256**   
   OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(10045) pkcs(4) pkcs-1(3) 3}

### Name forms

Certificates issued under the **1RPKI** contain the “Distinguished Name”, in X.500 format, for the issuer and the subscriber, set in the fields “Issuer Name” and “Subject Name” respectively, as described in section 7.1.2.

### Name constraints

The Issuing CAs adhering to this CP must ensure that only names pre-approved by IATA can be included in Server or Client certificates.

### Certificate policy object identifier

The Issuing CA must include mandatorily a policy object identifier (OID) in the Server certificates and optionally in the Client certificates.

The Issuing CA must disclose this information in its CPS.

### Usage of Policy Constraints extension

No stipulation for subscriber certificates. The CA can disclose additional stipulations in its CPS for CA certificates.

### Policy qualifiers syntax and semantics

No stipulation for subscriber certificates. The CA can disclose additional stipulations in its CPS for CA certificates.

### Processing semantics for the critical Certificate Policies extension

The “Certificate Policy” extension identifies the Policy that the **1RPKI** assigned explicitly to a certificate profile. Software Applications requiring a specific certificate profile to process a digital signature must check this extension in order to verify the suitability of the certificate for the intended purpose.

## CRL Profile

In general, CRLs generated under the **1RPKI** Trust Model must be compliant with RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002).

### Version number(s)

CRLs conforming to X.509 Version 2 are supported in the **1RPKI**.

### CRL Profile and CRL entry extensions

CRL must include the following minimum extensions, as defined by the above standard:

* CRL Number
* Authority Key Identifier
* Revocation date
* Reason code

## OCSP Profile

Issuing CAs are mandated to provide OCSP service at all types of TLS Certificates.

### Version number(s)

**1RPKI** provides support for Version 1 of RFC6960.

### OCSP extensions

No stipulation.

# Compliance Audit and Other Assessment

This section is included in this CP document only for standardization purposes. The reader must refer to the CPS published by the Issuing CA for all the relevant stipulations.

**In particular, IATA mandates that any Issuing CA adhering to this CP must follow the audit requirement for publicly trusted TLS certificates (Webtrust or equivalent).**

## Frequency or circumstances of assessment

*As stipulated in the CPS published by the Issuing CA.*

## Identity/qualifications of assessor

*As stipulated in the CPS published by the Issuing CA.*

## Assessor's relationship to assessed entity

*As stipulated in the CPS published by the Issuing CA.*

## Topics covered by assessment

*As stipulated in the CPS published by the Issuing CA.*

## Actions taken as a result of deficiency

*As stipulated in the CPS published by the Issuing CA.*

## Communication of results

*As stipulated in the CPS published by the Issuing CA.*

# Other Business and Legal Matters

This section is included in this CP document only for standardization purposes. The reader must refer to the CPS published by the Issuing CA for all the relevant stipulations.

## Fees

*As stipulated in the CPS published by the Issuing CA.*

### Certificate issuance or renewal fees

*As stipulated in the CPS published by the Issuing CA.*

### Certificate access fees

*As stipulated in the CPS published by the Issuing CA.*

### Revocation or status information access fees

*As stipulated in the CPS published by the Issuing CA.*

### Fees for other services

*As stipulated in the CPS published by the Issuing CA.*

### Refund policy

*As stipulated in the CPS published by the Issuing CA.*

## Financial Responsibility

*As stipulated in the CPS published by the Issuing CA.*

### Insurance coverage

*As stipulated in the CPS published by the Issuing CA.*

### Other assets

*As stipulated in the CPS published by the Issuing CA.*

### Insurance or warranty coverage for end-entities

*As stipulated in the CPS published by the Issuing CA.*

## Confidentiality of Business Information

*As stipulated in the CPS published by the Issuing CA.*

### Scope of confidential information

*As stipulated in the CPS published by the Issuing CA.*

### Information not within the scope of confidential information

*As stipulated in the CPS published by the Issuing CA.*

### Responsibility to protect confidential information

*As stipulated in the CPS published by the Issuing CA.*

## Privacy of Personal Information

*As stipulated in the CPS published by the Issuing CA.*

### Privacy plan

*As stipulated in the CPS published by the subordinate CA.*

### Information treated as private

*As stipulated in the CPS published by the Issuing CA.*

### Information not deemed private

*As stipulated in the CPS published by the Issuing CA.*

### Responsibility to protect private information

*As stipulated in the CPS published by the Issuing CA.*

### Notice and consent to use private information

*As stipulated in the CPS published by the Issuing CA.*

### Disclosure pursuant to judicial or administrative process

*As stipulated in the CPS published by the Issuing CA.*

### Other information disclosure circumstances

*As stipulated in the CPS published by the Issuing CA.*

## Intellectual Property Rights

*As stipulated in the CPS published by the Issuing CA.*

## Representations and Warranties

*As stipulated in the CPS published by the Issuing CA.*

### CA representations and warranties

*As stipulated in the CPS published by the Issuing CA.*

### RA representations and warranties

*As stipulated in the CPS published by the Issuing CA.*

### Subscriber representations and warranties

*As stipulated in the CPS published by the Issuing CA.*

### Relying party representations and warranties

*As stipulated in the CPS published by the Issuing CA.*

### Representations and warranties of other participants

*As stipulated in the CPS published by the Issuing CA.*

## Disclaimers of Warranties

*As stipulated in the CPS published by the Issuing CA.*

## Limitations of Liability

*As stipulated in the CPS published by the Issuing CA.*

## Indemnities

*As stipulated in the CPS published by the Issuing CA.*

## Term and Termination

*As stipulated in the CPS published by the Issuing CA.*

### Term

*As stipulated in the CPS published by the Issuing CA.*

### Termination

*As stipulated in the CPS published by the Issuing CA.*

### Effect of termination and survival

*As stipulated in the CPS published by the Issuing CA.*

## Individual notices and communications with participants

*As stipulated in the CPS published by the Issuing CA.*

## Amendments

*As stipulated in the CPS published by the Issuing CA.*

### Procedure for amendment

*As stipulated in the CPS published by the Issuing CA.*

### Notification mechanism and period

*As stipulated in the CPS published by the Issuing CA.*

### Circumstances under which OID must be changed

*As stipulated in the CPS published by the Issuing CA.*

## Dispute Resolution Procedures

*As stipulated in the CPS published by the Issuing CA.*

## Governing Law

*As stipulated in the CPS published by the Issuing CA.*

## Compliance with Applicable Law

*As stipulated in the CPS published by the Issuing CA.*

## Miscellaneous Provisions

*As stipulated in the CPS published by the Issuing CA.*

### Entire agreement

*As stipulated in the CPS published by the Issuing CA.*

### Assignment

*As stipulated in the CPS published by the Issuing CA.*

### Severability

*As stipulated in the CPS published by the Issuing CA.*

### Enforcement (attorneys' fees and waiver of rights)

*As stipulated in the CPS published by the Issuing CA.*

### Force Majeure

*As stipulated in the CPS published by the Issuing CA.*

## Other Provisions

*As stipulated in the CPS published by the Issuing CA.*

# Annex A: Glossary

1R ONE Record

1RPKI PKI issuing certificates approved to be used by ONE Record participants

1RID ONE Record ID

CA Certificate Authority or Certification Authority

CAA Certification Authority Authorization

CAB ”CA/Browser” as in “CAB Forum”

CMS Card Management System

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

CSR Certificate Signing Request

CT Certificate Transparency

DBA Doing Business As (also known as "Trading As")

DV Domain Validated

ETSI European Telecommunications Standards Institute

EU European Union

FIPS (US Government) Federal Information Processing Standard FQDN Fully Qualified Domain Name

FTP File Transfer Protocol

HSM Hardware Security Module

HTTP Hypertext Transfer Protocol

IANA Internet Assigned Numbers Authority

ICANN Internet Corporation for Assigned Names and Numbers IdM Identity Management System

IDN Internationalized Domain Name

ISSO Information System Security Officer (also CSO, Chief Security Officer)

IETF Internet Engineering Task Force

IGTF International Grid Trust Federation

ITU International Telecommunication Union

MICS Member‐Integrated Credential Service (IGTF) NIST National Institute of Standards and Technology OCSP Online Certificate Status Protocol

OID Object Identifier

ONE Record ID URL approved by IATA to publish or consume ONE Record services

OV Organization Validated

PAA Policy Approval Authority

PIN Personal Identification Number (e.g. a secret access code)

PKI Public Key Infrastructure

PKIX IETF Working Group on Public Key Infrastructure

RA Registration Authority

RFC Request for Comments (at IETF.org)

SAN Subject Alternative Name

SHA Secure Hashing Algorithm

SSL Secure Sockets Layer

TLD Top‐Level Domain

TLS Transport Layer Security

TSA Time Stamping Authority

TST Time‐Stamp Token

TTL Time To Live

UTC Coordinated Universal Time

X.509 The ITU‐T standard for Certificates and their corresponding authentication framework

1. These DNS names must be the list of unique FQDN extracted of the list of ONE Record IDs approved by IATA for this certificate [↑](#footnote-ref-1)
2. These URI names must be a set of unique URL representing the list of ONE Record IDs approved by IATA for this certificate [↑](#footnote-ref-2)