Revenue Public Key Infrastructure

Revenue CA

Certificate Policy

Document Version 2.0

Date May 2021

OID 1.2.372.980003.1.1.1.1.3

Revenue
Cáin agus Custaim na hÉireann
Irish Tax and Customs

Contents

1 Revision History

Version	Date	Author	Comments
Ver 1.1	7 April 2004	RSA/Revenue	Final version for publication.
Ver 1.2	20 August 2007	Revenue	Updated to take account of certs to be used by DoE and other Government Departments in the future.
Ver 2.0	May 2020	Atos/Revenue	Updated document to take account of new PKI provider software. New OID.

2 Purpose of this Certificate Policy Statement (CP)

The information contained in this CP is intended to inform those issued with Certificates by the Revenue CA of their rights and obligations. It also sets out how the Revenue CA will discharge its obligations to those persons.

Revenue reserves the right to add to, amend, or vary the terms of this agreement by publishing notice of such changes on its website and the continued use of the service will signify acceptance of the changes.

The framework in which the Revenue CA operates and its possible relationships with other proposed developments are shown in Figure 1.

Revenue PKI Framework

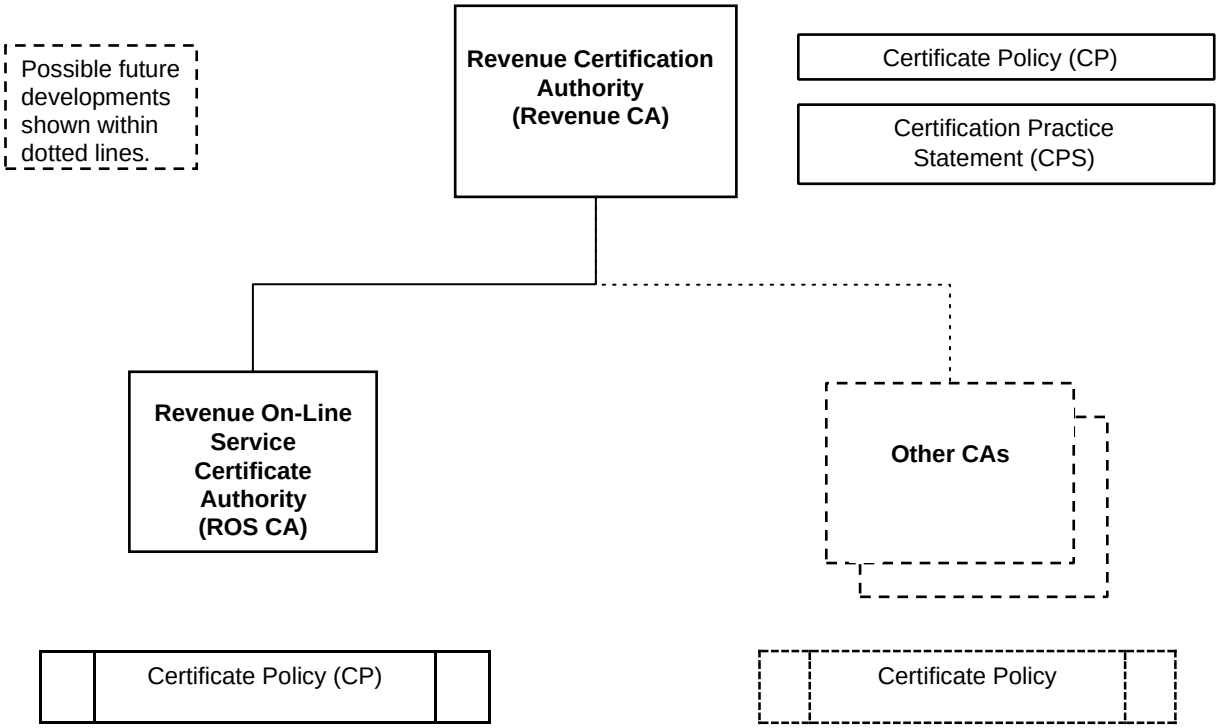

Figure 1 – Revenue PKI Framework

The relationship between the Revenue CA and the ROS CA is shown in Figure 2 on the following page.

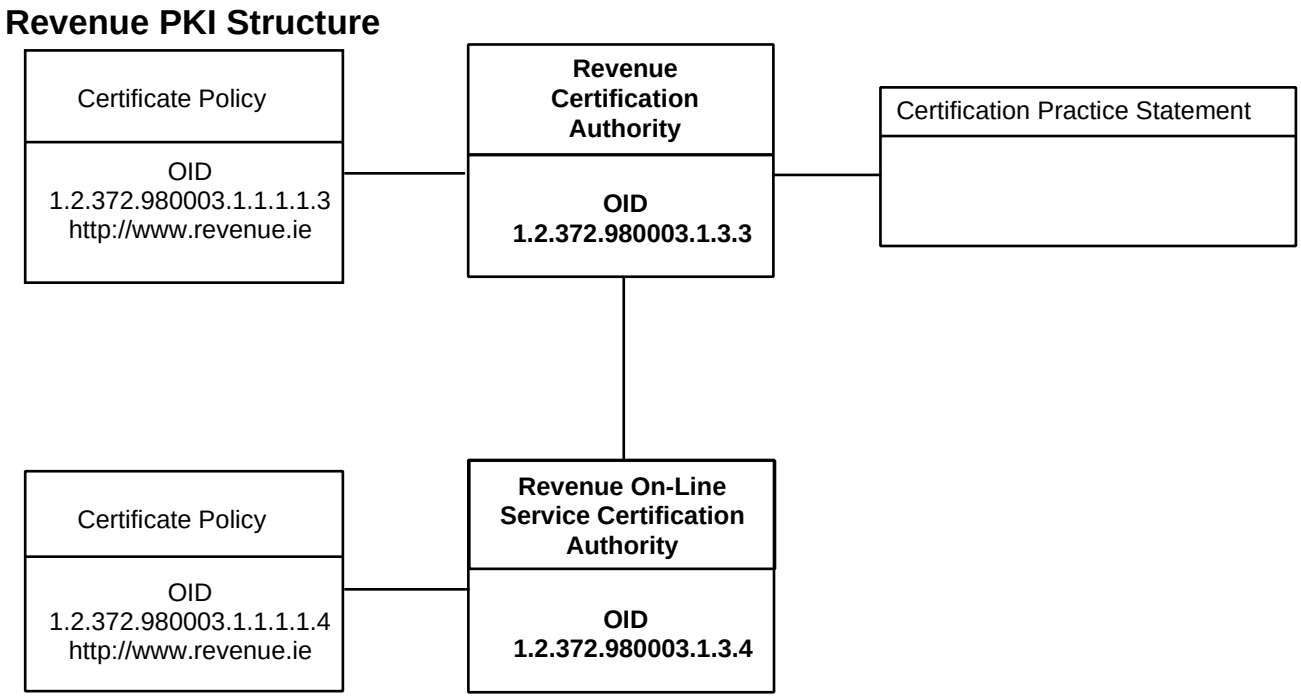

Figure 2 – Revenue PKI Structure

2.1 Revenue CA

The Revenue CA will issue under this CP, Certificates to the Revenue Online Services (ROS) CA whose uses will comply with the Conditions of Use (Section 3.1) that apply to those Certificates.

The Revenue CA operates under the Revenue PKI in accordance with the Revenue PKI Certificate Practice Statement.

3 Conditions of Use

3.1 Revenue CA private key

The private key of the Revenue CA should be used to:

- Sign the CA certificate (self-signed certificate)
- Sign the certificates of the Revenue Online CAs
- Sign the Authority Revocation List (ARL)

These uses are explicit in the extensions of the certificates.

3.2 Sub CA private key

The private key of the Sub CAs should be used to:

- Sign the certificates of the Approved Persons or Authorised Persons
- Sign the Certificate Revocation List (CRL)

These uses are explicit in the extensions of the certificates.

3.3 Revenue CA certificate

The Revenue CA certificate should be used to:

- Check the integrity of the public key of the Revenue CA (self-signed certificate)
- Check the origin and inheritance of the Revenue Online CAs
- Check the origin and integrity of the issuer Revenue CA ARL

3.4 Sub CA certificate

The certificates of the Sub CAs are intended for:

- Check the origin and integrity of the certificates issued by the Sub CAs
- Check the origin and integrity of the CRL delivered by the Sub CAs
- The Conditions of Use at section 3.2 set out the conditions that apply to Certificates issued by the ROS CA to an Approved Person or Authorised Person.

4 Policies for Certificates issued

The function of the policies is to provide guidelines for the following:

1. Generation, operational use, compromise, expiry, and revocation of Certificates issued by the Certificate Authority.
2. Security, mutual consistency, and effectiveness of the Certificate Authority operations.
3. Maintenance of the logical and physical elements of the Revenue's PKI.

The Revenue CA Policies are documented in the Certification Practice Statement.

This CP is also complemented by an annotated statement of the policy that appears in the Certificates issued by the Certificate Authority. That statement is known as the policy qualifier. This CP is also supported by supporting documents that are referenced throughout the Certification Practice Statement.

Unless otherwise stated, those documents are available on request by email to the ROS Helpdesk (roshelp@revenue.ie) .

5 Publishing Certificate Policy and Practice Documents

The Certificate Policy documents will be published on revenue web site – www.revenue.ie.

https://www.revenue.ie/en/online-services/support/data-and-security/ros-policy-and-practice-statement.aspx

Certification Practice Statement documents are available on request by email to the ROS Helpdesk (roshelp@revenue.ie) .

6 Amendment Procedure

6.1 Policy Approval Authority (PAA)

The responsibility for amending and approval of this document rests with the Revenue PKI Policy Approval Authority (PAA).

The PAA is responsible for setting Certificate Policy direction for Revenue's overall Public Key Infrastructure and includes representatives from the Offices of the Revenue Commissioners and other bodies as defined within the PAA Constitution.

6.2 Change

After a change to the Conditions of Use, the Certificate Policy or the Certificate Practice Statement has been approved the Revenue PAA will do the following:

1. Publish at the Revenue Web Site (see Section 5), this CP including the Conditions of Use.
2. Publish information advising the Revenue Online CAs with Certificates as to the effect of the change and its date of effect.
3. Cancel Certificates where the Approved Person or Authorised Person indicates that they no longer wish to abide by the new arrangements.

If an existing document requires re-issue, the change process employed is the same as for initial publication, as described above. Note that the new OID issued for a new document will have a new version number.

7 Certificates

7.1 Revenue CA Certificate Root Certificate

The Revenue CA will be a self-signed root certificate. The Revenue CA certificate will contain:

Field	Value
Version	"2" (representing X.509 V3)
Serial Number	An integer that acts as a unique identifier, generated by the CA
Signature Algorithm	Sha512WithRSAEncryption (1.2.840.113549.1.1.13) and Sha256withRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN=Revenue CA 2040, OU=Revenue On-Line Service, O=Revenue Commissioners, C=IE
Validity (From)	The date the certificate is valid from. (*date of issue*)
Validity (To)	The date the certificate is valid until. (*date of issue + 20 years*)
Subject	CN=Revenue CA 2040, OU=Revenue On-Line Service, O=Revenue Commissioners, C=IE
Subject Public Key Info	Key size is 4096
Authority Key Identifier (AKI)	SHA-1 hash of Revenue CA public key.
Subject key identifier (SKI)	SHA-1 hash of Revenue CA public key.

Basic constraints	CA: True, Maximum Path Length: Undefined
Key Usage	Key Cert Sign, CRL Signature
Certificate Policies	Certificate Policy OID: 1.2.372.980003.1.1.1.1.3 CP URL**:** www.revenue.ie

7.2 Revenue CA Certificates Issued to Revenue Online CAs

The Revenue CA certificate issued to the Revenue Online CA will contain:

Field	**Value**
Version	"2" (representing X.509 V3)
Serial Number	An integer that acts as a unique identifier, generated by the Revenue Online CA
Signature Algorithm	Sha512WithRSAEncryption (1.2.840.113549.1.1.13) and Sha256withRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN=Revenue CA 2040, OU=Revenue On-Line Service, O=Revenue Commissioners, C=IE
Validity (From)	The date the certificate is valid from. (*date of issue*)
Validity (To)	The date the certificate is valid until. (*date of issue + 10 years*)
Subject	CN=ROS CA 2030, OU=Revenue On-Line Service, O=Revenue Commissioners, C=IE
Subject Public Key Info	Key size is 4096
Authority Key Identifier (AKI)	SHA-1 hash of Revenue CA public key.
Subject key identifier (SKI)	SHA-1 hash of Revenue CA public key.
Basic constraints	CA: True, Maximum Path Length: 0
Key Usage	Key Cert Sign, CRL Signing
Certificate Policies	Certificate Policy OID: 1.2.372.980003.1.1.1.1.3 CP URL**:** www.revenue.ie