PORTIMA COMMUNITY ROOT AND SUBORDINATE CA 2019

CERTIFICATE POLICY

1.3.6.1.4.1.10438.1.3

V.1.0

PORTIMA

TABLE OF CONTENTS

VERSIONS

Version	Date	Major Changes
0.1	08/2019	Initial draft
0.2	10/2019	Updated draft
0.3	04/2020	Version number incremented to be aligned with CPS
1.0	08/2024	First approved version

1. Introduction

1.1 Overview

Portima SC/CV (hereinafter referred to as "Portima") Public Key Infrastructure (PKI) with Community Root and Subordinate CA 2019 provides certificates for security and trust services to support Portima's business partners.

This Certificate Policy (hereinafter referred to as "CP") is a statement regarding the policies that the Root and Community Certification Authority (CA) 2019 employs in issuing certificates for electronic transactions through Portima's network infrastructure.

This CP is based on the "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework" of the Network Working Group (RFC 3647).

This CP has to be read in combination with the applicable contractual documentation.

1.2 Document Name and Identification

This document is called "Portima Community Root and Subordinate CA 2019 - Certificate Policy".
The Policy ID for this CP is 1.3.6.1.4.1.10438.1.3

The present CP refers to the Certification Practice Statements named "Portima Community Root and Subordinate CA 2019 - Certification Practice Statement", with policy identifier
1.3.6.1.4.1.10438.1.4

1.3 PKI Participants

1.3.1 Certification Authorities

A Certificate Authority (herein referred to as "CA") is an authority trusted by Subscribers, Subjects and Relying Parties to create and sign certificates. Portima utilizes two CAs to issue, sign, publish, and revoke certificates for its Subscribers, Subjects and Relying Parties.

This Portima Community 2019 PKI is comprised of the following CAs:

- Portima Root CA (herein referred to as “Root CA”);
- Portima Community CA 2019 (herein referred to as “Subordinate CA”);

The roles and responsibilities of the Root CA are to

- Create self-signed root certificates
- Create and sign Subordinate CA certificates
- Revoke certificates it has issued
- Publish certificates to a certificate repository
- Issue CRLs for Subordinate CA certificates

The roles and responsibilities of the Subordinate CA are to

- Issue and sign certificates for Subjects
- Revoke certificates it has issued
- Publish certificates to a certificate repository
- Issue CRLs
- Publish CRLs

1.3.2 Registration Authorities

The Subordinate CA delegates tasks to a Registration Authority (hereinafter referred to as “RA”). Portima recognizes two types of the RAs:

- Portima RA (herein referred to as “PRA”); and
- Local Registration Authority or LRA (herein also referred to as “ delegated RA”);

Each RA has certain responsibilities with regard to the certificate enrollment process.

The PRA is responsible for validation of certificate application, validation of identity, and certificate registration for a Business Partner’s delegated RA. The PRA’s responsibilities do not include making certificate requests, issuing certificate or signing certificates.

PRA responsibilities is split over different persons (e.g. separating certificate application and identity validation from certificate registration) or might be done by a single person.

To facilitate the certificate enrollment process, the PRA delegates tasks such as certificate application, identity validation, and certificate authorization to a Business Partner’s delegated RA. These delegated RAs are formally nominated by a Business Partner’s management to administer their Subscriber community. Their role in the PKI is twofold:

- To validate the identity of their Subscribers and Entities; and

- To authorize the issuing of certificates for Subscribers and Entities.

1.3.3 Subject / Subscribers and Entities

The PKI considers a Subject / Subscriber as a natural person who uses X.509v3 certificates to authenticate or protect transactions through the Portima network. Employees, contractors, temporary personnel hired or engaged by a Business Partner, and Portima personnel who interact with the PKI in the scope of their normal responsibilities are considered Subscribers.

This PKI refers to an Entity such as a software application or application server.
Applications represent the business logic responsible for manipulating, storing, or forwarding data either internal or external to Portima's communications network.
Application Servers refer to the physical hardware and software (web servers or application servers) used to transact data between Business Partners or between Business Partners and Portima during day-to-day operations.

1.3.4 Relying Parties

A Relying Party is a recipient of a certificate who acts in reliance on that certificate. The Relying Party can be the Subject / Subscriber or an entity. They rely on certificates for authentication or trust services.

1.3.5 Certificate Repository

The Certificate Repository is a service that allows the certificates and certificate status to be retrieved upon demand. The following table summarizes the roles and responsibilities of a certificate repository:

Role	Description
Store Certificate	The Certificate Repository provides a capability to store a database of certificates.
Provide Certificate	The Certificate Repository provides a capability to look up specific certificates upon request and provide a copy of the certificate.
Confirm Status of Certificate	The Certificate Repository provides a capability to check the status of a certificate. This can be done as part of the "Provide Certificate" function (i.e. the status of the certificate is contained in the certificate when it is delivered)

Role	Description
	or as a separate function (i.e., returns a simple status flag rather than the entire certificate).

1.3.6 PKI Security Officers

To ensure the Root CA and Subordinate CA's integrity and security, Portima employs PKI Security Officers (herein referred to as "SO"). The overall responsibility of the SOs is to administer the implementation of the security practices within Portima.

As part of this PKI, the PKI SO's main role is the security of the CAs. In addition, they manage the day-to-day operations of the Subordinate CA, revoke RA and Subjects certificates in accordance with this CP and corresponding CPS.
PKI SOs are responsible for the installation, configuration, maintenance and, if necessary, recovery of the HSM (cf. Key Ceremony script).

1.3.7 PKI Registration Officers

The Registration Officers are the delegated RAs, fulfilling the registration roles and responsibilities (cf. section 1.3.2)

1.3.8 PKI Revocation Officers

PKI SOs and delegated RAs are Revocation Officers and they are responsible for revoking Subjects' certificates in accordance with this CP and corresponding CPS.

PKI SOs are the Revocation Officers responsible for revoking delegated RAs' certificates, in accordance to this CP and corresponding CPS.

1.3.9 PKI System Administrators

PKI system administrators are responsible for the installation, configuration, maintenance and, if necessary, recovery of Portima trustworthy systems for this PKI service management (except HSM), such as installation, configuration and maintenance of the certificate management database.

1.3.10 PKI System Operators

PKI systems operators are responsible for operating the PKI trustworthy systems on a day-to-day basis, such as backup and restoration of the certificate management database

1.3.11 PKI System Auditors

PKI System Auditors are authorized to view audit logs of the PKI trustworthy systems.

1.3.12 PKI Key Holders

In this PKI, there are 5 key holders (cf. Key Ceremony Script).

1.4 Certificate Usage

1.4.1 Appropriate Certificate Use

The certificate usages for the Root CA are

- To generate a self-signed root CA certificate
- To issue and sign the certificates of the subordinate CA
- To sign the CRL of revoked subordinate CA certificates

The certificate usages for the Subordinate CA are

- To issue and sign the certificates of Subjects
- To sign the CRL of revoked Subjects' certificates

The certificate usages for Subjects are

- Authentication
- Information integrity
- Confidentiality
- Access control
- Non repudiation

1.4.2 Prohibited certificate use

Digital certificates issued by this PKI may not be used:

- For usages other than those described in previous section;
- By External Parties with no contractual relationship with Portima's Business Partners or without a Business Partners obtaining prior agreement from Portima;

- By Relying Parties conducting transactions having no relationship to the services and/or applications provided by Portima.

1.5 Policy Administration

1.5.1 Organization Administering the document

Portima as the Certification Authority for this PKI maintains, registers, revises, and interprets this CP.

1.5.2 Contact Person

All questions and comments concerning this document must be addressed to:

Portima PKI Security Officers
Chaussée de la Hulpe 150
1170 Bruxelles
Belgium
Tel: +32 (0)2 661 44 11
Fax: +32 (0)2 661 44 00
Email: security@portima.com

1.5.3 CP Approval Procedure

Significant changes of this CP require an ad-hoc meeting of Portima CODIR for review and approval.

If a change is determined by Portima to have a material impact on the Subjects/Subscribers, Portima will assign a new version number and may, at its sole discretion, change the document name.

Each time the CP is modified with the approval of Portima CODIR, the date of the modification is updated and the version number is incremented.
A new release of the present CP is published after updates to this document.
No amendment will have retroactive effect on the certificates already issued.

1.6 Definitions and Acronyms

Access Control Database (ACD)

The Access Control Database is a repository that contains the Subject's privileges.

Application

The Application is the software used by Subjects and developed by Portima that has been enabled for functionalities such as certificate lifecycle management, key pair generation and protection, and digital signature. BRIO4YOU and AS/Web are considered as "Applications".

Certificate

The certificate is a digital object that binds a Subject's name to a public key. The certificate is signed by the issuing subordinate CA.

Certificate Policy (CP)

A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certificate Revocation List (CRL)

A CRL is the basic mechanism by which the CA distributes status information about a certificate. The CRL contains a list of serial numbers of certificates that should not be trusted anymore. It is a tamper resistant digital object because it is digitally signed by the CA.

Certification Authority (CA)

The CA is the collection of hardware, software, and people who operate it. The CA performs four basic operations:

- Issues certificates (i.e., creates and signs them).
- Maintains certificate status information and issues CRLs
- Publishes certificates and CRLs
- Maintains status information about expired or revoked certificates that it issued.

Portima owns and operates the Root and subordinate CA.

Certification Path

An ordered sequence of certificates from the initial object in the path to the final object in the path.

Certification Practice Statement (CPS)
A statement of the practices, which a CA employs in issuing and managing certificates.

CODIR
Portima CODIR is the management committee of Portima.

Distinguished Name (DN)
The certificate holder is expressed as an x.500 Distinguished Name (in accordance with industry standards) which describes a unique entry in the repository where the certificate is held.

Identity Provider (IP)
The IP is the system ruling the authentication and authorization within a Portima application. It relies on the ACD.

Issuer
Portima who owns and operates the CA acts as issuer of public key certificates.

Local Registration Authority (LRA)
To facilitate the certificate enrollment process, Portima delegates tasks such as certificate application, identity validation, and certificate authorization to a Business Partner's LRA. These delegated RAs are formally nominated by a Business Partner's management to administer their Subscriber community

Personal Identification Number (PIN)
A PIN having a minimum length of four (4) alphanumeric characters and a maximum length of ten (10) alphanumeric characters is used to protect access to the Subject's private keys.

Portima
Owner and operator of this PKI

Public Key Infrastructure (PKI)
The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke certificates. A PKI is based on public-key cryptography.

Registration Authority (RA)
The RA collects and verifies identity information of the Subjects before a request for a certificate is submitted to the CA.

RA management system
The RA Management System is a software used by delegated RA that has been enabled for typical RA operations such as Subject registration with face-to-face

(including eID recording), Subject onboarding authorization, visual controls, revocation requests. AS/Web is considered as an "RA management system".

Relying Party — A Relying Party is a recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate.

Repository — A repository accepts certificates and certificate revocation notice and status from one or more CAs and makes them available to relying parties that need them to implement security services.

Subject — A Subject is a natural person (e.g. broker) or an entity (e.g. application server).

Subscriber — Subscribers are the brokers who have subscribed to services with Portima. Some Subscribers act as delegated RA for the other employees of their broker company or office.

2. Publication and Repository Responsibilities

This section describes provisions applicable to the CA's obligations to publish information in respect of its practices, the frequency of such publication, access control in respect of published information and requirements governing the use of repositories.

2.1 Repositories

Portima owns and operates several repositories

- A repository (Identity Provider) to store Subject's credentials in an appropriate format to respect privacy
- A repository containing the certificates and CRLs (Certificate Management database)

2.2 Publication of Certificate Information

Brokers, Companies, and External Parties using this PKI are provided with the Root and Subordinate CA public certificates and the corresponding hash of the public keys.

Subjects' certificates are published in a Certificate Management database immediately after issuance.

When revoked, subCA certificates are published in CRL:
http://crl.portima.be/crl/rootCommunity.crl

When revoked, Subjects' certificates are published in the CRL (available 24 hours a day, 7 days per week):
http://crl.portima.be/crl/community2019.crl

2.3 Time and Frequency of Publication

2.3.1 Root CA

Once created, Subordinate CA' certificates are published to the repository within 1 hour.

CRLs are published within 24 hours after being issued and are issued every 180 days.

2.3.2 Subordinate CA

Once created, Subjects' certificates are published immediately to the repository.
CRLs are published less than 8 hours after being issued by the Subordinate CA or at least, once a day.

2.4 Access control on published information

This CP is available to all Subjects/Subscribers who use Portima PKI. The certificate repository and certificate status in the Identity Provider will be accessible to Portima RA, the delegated RA, Users to enable verification of all certificates.

3. Identification and Authentication

3.1 Naming

3.1.1 Type of names

The Root CA and Subordinate CA use an X.500 Distinguished Name format for X500 Subject and Issuer name fields.

The following table describes the mandatory naming attributes for LRA, Subscribers, and Application Server certificates:

Entity	Attribute	Description
LRA	Name	Full name of the delegated RA where the name is not the function or department
	Company	Unique organizational identity
	Country	Country of the requestor
	E-mail address	RFC-822 mail box of the delegated RA
	UserID	Unique UserID of the physical person
	Office ID	Broker's unique Office ID
PSO	Name	Portima Root CA Security Officer [#]
	Surname	Full name of the PSO [First name Last name]
Subscribers	Name	Full name of the Subscriber where the name is not the function or department
	Company	Unique organizational identity
	Country	Country of the supplicant
	E-mail address	RFC-822 mail box of the Subscriber
	UserID	Unique UserID of the physical person
	Office ID	Broker's unique Office ID
Application Servers	Master Server	Application Server name
	Master Service	Application Server Service
	IP Address	Application Server's IP address
	IP Port	Application Server's IP Port

3.1.2 Uniqueness of names

The Root and Subordinate CA guarantee the uniqueness of the Distinguished Name information entered in the subject field of the certificate within the X.500 name space for which it has been authorized

The set of names in accordance with this CP is unique within the set of all Subscriber names in the Portima PKI thanks to a unique USerID.

3.1.3 Anonymity of Subjects

Subjects cannot be anonymous.

3.1.4 Rules for Interpreting Various Name Forms

Only names in the form of X.500 Distinguished Names are used, cf. profile of certificates in §7.1 of CPS.

3.1.5 Recognition, authentication and role of trademarks

The PRA authenticates the names of a delegated RA, Users, Application Servers, and Applications within the Portima name space. A delegated RA authenticates the names of his Subscribers and Entities within the Portima name space.
Portima's Legal Counsel ensures trademarks used in Subscriber and Entity certificates can be legitimately used and do not infringe on any Intellectual Property Rights.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

N/A.

3.2.2 Authentication of organization identity

Any existing contract between Portima and the Business Partner constitutes authentication of the organization's identity.

3.2.3 Authentication of individual identity

The following tables describes authentication of individual identity including entities within the Portima PKI.

Validation of Identity	Method
LRA (Delegated RA)	Face-to-face registration with the PRA at which time the delegated RA's identity is verified against a national identity card.
Subscriber	Business Partner's delegated RA validates the identity of a Subscriber.

Entity	Business Partner's delegated RA or System Administrator validates the identity of the Application or Application Server. Applications may be identified through its name or other mechanisms that uniquely identifies the application. Application Servers may be identified through their server name, URI and/or IP address.

3.2.4 Non verified subscriber information

N/A

3.2.5 Validation of Authority

N/A.

3.2.6 Criteria for interoperation

N/A

3.3 Identification and Authentication for re-key requests

N/A

3.4 Identification and Authentication for revocation requests

The identification and authentication for a revocation request is based on a signed Certificate Revocation Request (CRR) submitted by either the Business Partner's Manager or Supervisor, delegated RA or Portima RA. This procedure applies to Subscribers and Entities.

4. Certificate Life-Cycle Operational Requirements

For detailed information regarding certificate life-cycle procedures, please see the CPS.

4.1 Subjects

4.1.1 Summarized Requirements for Canonical Certificates of Subscribers

Prior to commencing the certificate application process, the delegated RA must decide which Subscribers have a business needs to access Portima's network and application resources.
The validation process should be based on a face-to-face meeting between the delegated RA and the Subscriber. The identity validation should be based on verification of the Subscriber's national identity card, passport or driver licence. It is recommended a photocopied photo identifications be stored at the Business Partner premises for audit purposes. The delegated RA has the right to require the subscriber to fill in a complete certificate application form.
The registration process relies on an ACD. This database contains pre-loaded information about the delegated RA's Subscribers. Delegated RA can access it after authentication to Portima web service.

Once authenticated, an encrypted session is established between the delegated RA's workstation and Portima web service. The encrypted session ensures all information communicated between the two systems is secure.
To ensure information privacy and confidentiality, the delegated RA can only view and browse records for Subscribers assigned to his OfficeID(s). The delegated RA selects all Subscribers (via the OfficeID) who he has authorized to receive a Portima certificate.

The delegated RA must verify the information (last name, first name, mobile number and email address) presented on the form against the Business Partner's internal records. Discrepancies between the Business Partner's records and information stored in the ACD must be reported to Portima immediately. Portima will correct any inconsistencies in a timely manner.
If there are no discrepancies the delegated RA changes the status of the user in the ACD which triggers the authorization for the Subscriber to download his certificate.

Once the authorization process has been successful, an email is automatically sent to the delegated RA and/or the Subscriber. This email contains the Subscriber's UserID (P1). The password (P2) is displayed on delegated RA's PC screen.
The Subscriber must have P1 and P2 in his possession prior to requesting his certificate.

With the above information, the delegated RA accesses Portima's webservice used exclusively for certificate requests and downloads.
The communication channel between the Subscriber's workstation and web service is protected through encryption so that the UserID (P1) and Password (P2) are never sent over the network in plain text.

The Subscriber inputs his UserID (P1) and Password (P2) into the appropriate form fields. The information is verified against the ACD for authenticity. A successful verification automatically triggers the creation of the Subscribers key pairs on the workstation.

A certificate request is automatically generated and sent to the Subordinate CA. During the request process, the Subscriber's private key is encrypted and embedded in the request. During the normal processing of the request, the private keys are stored in the key archive at Portima.

The Subordinate CA creates and signs the certificate. The certificate is automatically downloaded to the Subscriber's workstation. The Subscriber is prompted to input a PIN code. This PIN code protects the private key from access by unauthorized parties. Therefore, it is strongly recommended that the PIN code be at least six (6) characters long and be kept secret. Immediately after the PIN code entry, the certificate is automatically stored in the appropriate certificate store.

The Subscriber should verify the accuracy of the information contained in the certificate and compare the Subordinate CA's fingerprint against the one published by Portima. Any discrepancies with the information contained in the certificate or fingerprint must be immediately reported (by email) to a PSO.

The Subscriber is ready to begin accessing Portima's Application Servers and Applications.

Note: Should a processing error occur during the certificate request, the delegated RA must contact the Portima support (+32 2 661 44 22) who will take the necessary steps to resolve the issue.

4.1.2 Summarized Requirements for Mobile Certificates of Subscribers

If the Subscriber is already a user of the PKI, he has already been registered by the delegated RA.
Otherwise, the registration process is similar to the one for canonical certificates (cf. previous section) and registration is done by the delegated RA.

Then, if the Subscriber is already a user of the PKI, he authenticates against the ACD with his canonical certificate. A successful verification of his identity automatically triggers the creation of the Subscribers key pairs on the workstation of the delegated RA. A certificate request is automatically generated and sent to the Subordinate CA.

If the Subscriber is not yet a user of the PKI, the delegated RA verifies the Subscriber's identity. Then the delegated RA triggers the creation of the Subscribers key pairs on the delegated RA's workstation. A certificate request is automatically generated and sent to the Subordinate CA.
The Subordinate CA creates and signs the certificate.

On the delegated RA's workstation screen, the QRcode (partial URL with unique ID) to download the PKCS#12 is displayed.

Partial URL contains GUID of the Subscriber and unique GUID generated for this PKCS#12.

From his tablet or smartphone where he pre-installed Portima certificate-enabled application, the Subscriber can download the PKCS#12 using the QRcode (partial URL with unique ID) that he scanned from the workstation screen, together with the out of band DC code (Download Code) that he received by email or SMS.

The DC code is a code of six (6) numbers that is valid until the expiration or revocation of the corresponding PKCS#12. It can be resent to the Subscriber by email or SMS, as many times as needed until it is valid.
Portima certificate-enabled mobile applications already contain the root CA certificate and the Subordinate CA certificate so the certification path can be validated.

4.1.3 Requirements for Smart card based certificates of PSO

See CPS.

4.1.4 Requirements for Certificates for Applications or Application Servers

See CPS.

4.2 Key pair and certificate usage

See section 1.4

4.3 Certificate renewal

A certificate has a limited validity period. Prior to the end of this validity period, the delegated RA and Subscriber must renew the certificate to ensure continued access to Portima network resources and applications. No other circumstances warrant a certificate renewal.

4.4 Certificate re-key

N/A because there is no re-key of Subjects' certificates. Subjects have to request the issuance of a new certificate.

4.5 Certificate modification

N/A because certificate modification is not authorized under this CP and related CPS.
To correct certificate data, the Subscriber / delegated RA must revoke the certificate following the procedures described in the CPS and request a new certificate with the corrected data.

4.6 Certificate revocation and suspension

There is no certificate suspension under this CP and related CPS.

A Subscriber may request revocation of a certificate at any time for any reason. Portima or the delegated RA may also revoke a certificate upon failure of the Subscriber to meet its obligations under the CP, CPS, or any other agreement, regulation, or law applicable to the certificate. This includes revoking a certificate when a suspected or known compromise of the private key has occurred.
A Subscriber must request the revocation of a certificate under the following conditions:

- Whenever any material information on the certificate changes or becomes obsolete;

- Whenever the private key, or the media holding the private key, associated with the certificate is known or suspected of being compromised;
- Whenever a delegated RA or a Subscriber is no longer affiliated with a business partner's organization;
- Whenever a delegated RA or Subscriber is no longer in control of his PIN code;
- When his computer, mobile or tablet is being stolen or lost or decommissionned

Portima RA or the delegated RA will revoke a certificate under the following conditions:

- Upon request of the Subscriber or delegated RA;
- Upon failure of the Subscriber to meet its material obligations under the CP, CPS or any other agreement, regulation, or law applicable to the certificate;
- If knowledge or reasonable suspicion of compromise is obtained;
- If Portima determines that the certificate was not properly issued; or
- Whenever the delegated RA or Subscriber passes away;
- Whenever Subscriber's mobile or tablet is being stolen, lost or decommissioned.

Certificate revocation and suspension procedures for Subscribers and Entities are described in the CPS.

4.7 Certificate status service

See section 2.3

4.8 End of Subscription

N/A

4.9 Key escrow and key recovery

N/A for Subjects

5. Facility, Management and operational Controls

For detailed information regarding facility, management and operational controls, please see the CPS

6. Technical Security Controls

For detailed information regarding technical security controls, please see the CPS.

7. Certificate, CRL and OCSP profiles

For detailed information regarding Subject's certificate and CRL profiles, please see the CPS
There is no OCSP service as part of this PKI.

8. Compliance audit and other assessments

8.1 Frequency and circumstances of assessment

Services of this PKI can be audited by an independent external auditor, upon request of Portima's shareholders or Insurance Control Bodies or Portima CODIR.

8.2 Identity/qualifications of assessor

A competent independent professional firm that complies with appropriate national and international standards and codes of practice can qualify as an independent external assessor.

8.3 Assessor's relationship to assessed entity

The relationship between Portima and its assessors is limited to contractual relationship between parties.

8.4 Topics covered by assessment

The audit will determine the compliance of the CA services with this CP and the corresponding CPS. It will determine the business risks of non-compliance to the CP and corresponding CPS in accordance with the agreed control objectives.

8.5 Actions taken as a result of deficiency

The CA will undertake to resolve any deficiencies or non-conformities identified as a result of an audit within an agreed timescale dependent upon the severity of the risks involved.

8.6 Communication of results

For security reasons, the audit results are not published or provided to parties external to Portima.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Not applicable.

9.1.2 Certificate access fees

Not applicable.

9.1.3 Revocation or status information access fees

Not applicable.

9.1.4 Fees for other services such as policy information

Not applicable.

9.1.5 Refund policy

Not applicable

9.2 Financial Responsibilities

Not applicable.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following information is considered as confidential:

- Information collected by the RA to identify and authenticate Subjects, Application Servers, and Applications.
- PKI Contingency and Business Continuity plans.
- Subjects' private key, Application Servers' key, and Application's private key and related key activation data (PIN).
- Root and subordinate CA's private key.
- Root and subordinate CA and RA's audit trail records.

9.3.2 Information not within the scope of confidential information

Certificates and the present CP are not considered as confidential but they should only be disclosed to the entities that are part of the PKI.

Certificates and the present CP cannot contain confidential information or privacy sensitive information.

9.3.3 Responsibility to protect confidential information

Entities allowed to access confidential information cannot disclose them.

9.4 Privacy of personal information

9.4.1 Privacy plan

Portima's privacy plan protects sensitive information in accordance with all European Union directives, regulations and Belgium laws.
Personal data handled by Portima as part of the Application usage are archived for the longest period hereafter:

- Certificate validity period + 7 years
- The duration required by the business requirements related to the trusted services provided by Portima.

9.4.2 Information treated as private

Information pertaining to a Subject is treated as private.

9.4.3 Information not deemed private

Public information is not deemed as private.

9.4.4 Responsibility to protect private information

Private information is afforded the appropriate level of protection in accordance with all European Union directives, regulations and Belgium laws.

9.4.5 Notice and Consent to use private information

When necessary, a notice and consent to use private information is used.

9.4.6 Disclosure pursuant to judicial or administrative process

The CAs and RA are allowed to release confidential information based on a Belgian court order that is duly signed by a competent judge.

9.4.7 Other information disclosure circumstances

There are no other circumstances for the CAs and RA to release their confidential information.

9.5 Intellectual Property Rights

This CP is the absolute property of Portima and must not be copied, modified or reproduced without Portima's prior written consent.
No right or interest in any intellectual property rights are granted to Relying Parties under this CP. All rights in intellectual property are reserved to the CA or the RA as set out in the contract between them.

9.6 Representations and warranties

Not stipulated

9.7 Disclaimers of warranties

Not stipulated

9.7.1 Limitations of Liability

The CAs' liabilities are set out in the contract between Portima and the Business Partner. Other liability issues are dealt within contracts between relevant parties.

9.8 Indemnities

See contract.

9.9 Term and Termination

Not stipulated.

9.10 Individual notices and communications with participants

Not stipulated

9.11 Amendments

Portima may amend this CP at any time. No amendment will have retrospective effect.
Significant changes of the corresponding CPS require an ad-hoc meeting of Portima CODIR for review and approval. During this ad-hoc meeting, PKI Security Officers inform members of Portima CODIR of intended changes, their impact on the existing CP, and his recommended actions. A decision is taken by Portima CODIR to approve changes.

9.12 Dispute Resolution Provisions

Before taking formal legal steps to resolve a dispute in respect of Portima, a Subject must first raise the matter directly with Portima, which will endeavour promptly to resolve the dispute.

9.13 Governing Law

This CP and the relationships between the CA, Subscribers, Subjects and Relying Parties are subject to and will be interpreted in accordance with the REGULATION (EU) 910/2014 and the laws of Belgium.

9.14 Compliance with applicable law

Please refer to 9.13

9.15 Miscellaneous provisions

Any contract or agreement referring to this CP will specify that the terms of this CP will continue to apply in the event of severance, survival, merger or notice affecting any party.

9.16 Other provision

Usage of this PKI does not and shall not discriminate on the basis of race, color, religion (creed), gender, gender expression, age, national origin (ancestry), disability, marital status, sexual orientation, or military status, in any of its activities or operations.