PORTISIGN™ POLICIES AND STATEMENTS

USERS CA 10 AND USERS CA 11 - QUALIFIED CERTIFICATES

CERTIFICATE POLICY

1.3.6.1.4.1.10438.3.2.4.10.1

v1.3 (1.3.6.1.4.1.10438.3.2.4.10.1.1.3)

TABLE OF CONTENTS

1. INTRODUCTION ................................................................................................................. 5
   1.1 OVERVIEW .................................................................................................................. 5
   1.2 DOCUMENT NAME AND IDENTIFICATION ......................................................... 5
   1.3 PKI PARTICIPANTS ................................................................................................. 5
   1.4 CERTIFICATE USAGE ............................................................................................ 9
   1.5 POLICY ADMINISTRATION ....................................................................................... 9
   1.6 DEFINITIONS AND ACRONYMS ............................................................................. 10

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES ............................. 13
   2.1 REPOSITORIES ........................................................................................................ 13
   2.2 PUBLICATION OF CERTIFICATE INFORMATION ........................................ 13
   2.3 TIME AND FREQUENCY OF PUBLICATION .................................................. 13
   2.4 ACCESS CONTROL ON PUBLISHED INFORMATION ....................................... 14

3. IDENTIFICATION AND AUTHENTICATION ................................................. 15
   3.1 NAMING .................................................................................................................. 15
   3.2 INITIAL IDENTITY VALIDATION ........................................................................... 15
   3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS ........... 16
   3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS .... 16

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS .......................... 17
   4.1 SUBJECTS .............................................................................................................. 17
   4.2 KEY PAIR AND CERTIFICATE USAGE ............................................................... 17
   4.3 CERTIFICATE RENEWAL ..................................................................................... 17
   4.4 CERTIFICATE RE-KEY ........................................................................................... 17
   4.5 CERTIFICATE MODIFICATION ............................................................................. 17
   4.6 CERTIFICATE REVOCATION AND SUSPENSION ............................................. 17
   4.7 CERTIFICATE STATUS SERVICE .......................................................................... 17
   4.8 END OF SUBSCRIPTION ......................................................................................... 17
   4.9 KEY ESCROW AND KEY RECOVERY ..................................................................... 17

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS .................. 18

6. TECHNICAL SECURITY CONTROLS .............................................................. 18

7. CERTIFICATE, CRL AND OCSP PROFILES ............................................... 19
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS.......... 20
8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT........... 20
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR ..................... 20
8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY ............. 20
8.4 TOPICS COVERED BY ASSESSMENT ................................ 20
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY ............... 20
8.6 COMMUNICATION OF RESULTS .................................... 20

9. OTHER BUSINESS AND LEGAL MATTERS.................... 21
9.1 FEES ........................................................................ 21
9.2 FINANCIAL RESPONSIBILITIES .................................... 21
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION ........... 21
9.4 PRIVACY OF PERSONAL INFORMATION ....................... 21
9.5 INTELLECTUAL PROPERTY RIGHTS ............................. 22
9.6 REPRESENTATIONS AND WARRANTIES ......................... 22
9.7 DISCLAIMERS OF WARRANTIES ................................. 22
9.8 INDEMNITIES .......................................................... 22
9.9 TERM AND TERMINATION .......................................... 22
9.10 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS .......... 23
9.11 AMENDMENTS ........................................................ 23
9.12 DISPUTE RESOLUTION PROVISIONS ............................ 23
9.13 GOVERNING LAW .................................................... 23
9.14 COMPLIANCE WITH APPLICABLE LAW ....................... 23
9.15 MISCELLANEOUS PROVISIONS ............................... 23
9.16 OTHER PROVISION .................................................. 23
## VERSIONS

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Major Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>03/2015</td>
<td>Initial draft</td>
</tr>
<tr>
<td>0.2</td>
<td>03/2016</td>
<td>Updates after production key ceremony of Feb 24 and 25, 2016</td>
</tr>
<tr>
<td>0.3</td>
<td>03/2017</td>
<td>Updates after pre-audit eIDAS in Dec 2016</td>
</tr>
<tr>
<td>1.0</td>
<td>13/04/2017</td>
<td>First published version approved by COMDIR</td>
</tr>
<tr>
<td>1.1</td>
<td>23/05/2017</td>
<td>Updates after stage 1 audit eIDAS on April 24 and 25, 2017</td>
</tr>
<tr>
<td>1.2</td>
<td>20/06/2017</td>
<td>V 1.2 approved by COMDIR - Published</td>
</tr>
<tr>
<td>1.3</td>
<td>23/08/2017</td>
<td>Updates after stage 2 audit eIDAS in July 2017</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V 1.3 approved by Steering Commitee PortiSign - Published</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

1.1 Overview
Portima s.c.r.l. c.v.b.a. (hereinafter referred to as “Portima”) Public Key Infrastructure (PKI) for PortiSign™ provides qualified certificates for electronic signature of documents. The PortiSign™ Certificate Policy (hereinafter referred to as “CP”) is a set of rules and policies followed by the PortiSign Certification Authorities (CA) when issuing and managing these certificates. 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 “PortiSign™ Policies and Statements - Users CA 10 and Users CA 11 - Qualified Certificates - Certificate Policy”. The Policy ID for this CP is 1.3.6.1.4.1.10438.3.2.4.10.1

The present CP refers to the Certification Practice Statements named “PortiSign™ Policies and Statements - Users CA 10 and Users CA 11 - Qualified Certificates - Certification Practice Statement”, with policy identifier 1.3.6.1.4.1.10438.3.2.4.10.2

A PKI Disclosure Statement also exists. Its name is PortiSign™ Policies and Statements - Users CA 10 and Users CA 11 - Qualified Certificates - PKI Disclosure Statement” and its policy identifier is 1.3.6.1.4.1.10438.3.2.4.10.3

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 three CAs to issue, sign, publish, and revoke certificates for its Subscribers, Subjects and Relying Parties.

The PortiSign™ PKI is comprised of the following CAs:
- PortiSign Root CA (herein referred to as “Root CA”);
- PortiSign Users CA 10 for qualified certificates (herein referred to as “Subordinate CA 10”);
- PortiSign Users CA 11 for qualified certificates (herein referred to as “Subordinate CA 11”).
- PortiSign Users CA 1 2016 for advanced certificates and general purpose certificates that are necessary for PortiSign PKI operations (e.g. certificates of Security Officers)
- PortiSign Users CA 2 2016 for advanced certificates and general purpose certificates that are necessary for PortiSign PKI operations (e.g. certificates of Security Officers)

Note : The PortiSign Users CA 1 2016 and PortiSign Users CA 2 2016 are ruled by specific CP and CPS documents:
- Portisign Certificate Policy (OID: 1.3.6.1.4.1.10438.3.2.1)
- PortiSign Certification Practice Statement (OID: 1.3.6.1.4.1.10438.3.2.2)
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 table below summarizes the roles and responsibilities of the Subordinate CA 10 and Subordinate CA 11 for qualified certificates in PortiSign PKI:

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue (Sign) Certificate</td>
<td>The CA equipment has a capability to apply its CA signature to new certificates being issued. This signature assures recipients that the certificate was issued in accordance with the CA's published policy.</td>
</tr>
<tr>
<td>Revoking certificates</td>
<td>The CAs are responsible for revoking a Subject’s certificate.</td>
</tr>
<tr>
<td>Provide Certificate to Subjects</td>
<td>The sub CA equipment has a capability to deliver the certificate to the Subject.</td>
</tr>
<tr>
<td>Publish Certificate</td>
<td>The CA equipment has a capability to submit the certificate to the Certificate Repository where it will be made available to whoever needs a copy.</td>
</tr>
<tr>
<td>Revoke Certificate</td>
<td>The CA equipment has a capability to carry out a certificate revocation by marking the certificate as revoked in the certificate repository.</td>
</tr>
</tbody>
</table>

1.3.2 Registration Authorities

The Subordinate CAs delegate some registration tasks to delegated Registration Authorities but Portima remains the Registration Authority of PortiSign PKI. Each delegated RA is responsible for

- meeting face-to-face (F2F) with their customers (hereafter called the “Subject”) in order to pre-validate their identity
- saving their customers’ eID and mobile phone number
- providing access to the Application

Portima is providing tools to the delegated RA to process and store any relevant registration and revocation information.

The delegated RA has the following roles:

- Registration of the Subject of the certificate;
- Subjects’ certificate revocation.

But Portima as the RA of PortiSign PKI is the only one to have the role to validate the identity of the Subjects.

1.3.3 Subscribers

Subscribers are the insurance brokers who have subscribed services with Portima.
1.3.4 Subjects

This PKI considers a Subject of a certificate as a natural person who uses X.509v3 certificates to electronically sign a document within an Application.

The table below summarizes the roles and responsibilities of the Subjects:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate Certificate Request</td>
<td>The Subject generates a certificate request.</td>
</tr>
<tr>
<td>Generate Private Keys</td>
<td>The Subject generates his private keys using the SKB of his mobile device</td>
</tr>
<tr>
<td>Create Certificate Signing Request (CSR)</td>
<td>The SKB generates a CSR that contains the Subject's claimed identity and the public key the Subject wants to be bound to that identity.</td>
</tr>
<tr>
<td>Install &amp; Store Private Key</td>
<td>The private key is stored in the SKB and protected by a five (5) digit PIN code.</td>
</tr>
<tr>
<td>Install/Store Certificate</td>
<td>The certificate is stored in the Certificate Management database</td>
</tr>
<tr>
<td>Sign with Private Key</td>
<td>The Subject can sign with his private key documents within PortiSign™–enabled applications</td>
</tr>
<tr>
<td>Present Certificate to Others</td>
<td>The Portima cryptographic software has a capability to send the Subject's certificate to applications, servers, or relying parties who need to know the Subject's identity and public key. The presenting of a certificate is equivalent to claiming an identity. The ability to pass a proof of possession test is needed to know that the certificate being presented is, in fact, the Subject's own certificate, thereby proving the identity claim.</td>
</tr>
</tbody>
</table>

1.3.5 Relying Parties

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. The Relying Party can be the Subject, a Subscriber, another natural person, a legal entity, CAs, RAs, a software application, or an application server. They rely on certificates for digital signature verification.

The table below summarizes the roles and responsibilities of relying parties:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validate Certificate</td>
<td>The Relying Party is able to validate the certificate. Among other controls, this might be done by verifying the status of the certificate.</td>
</tr>
<tr>
<td>Verify Signatures</td>
<td>The Relying Party has the capability to use the certificate to check the Subject’s signature.</td>
</tr>
</tbody>
</table>

1.3.6 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:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store Certificate</td>
<td>The Certificate Repository provides a capability to store a database of certificates.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Provide Certificate</td>
<td>The Certificate Repository provides a capability to look up specific certificates upon request and provide a copy of the certificate.</td>
</tr>
<tr>
<td>Confirm Status of Certificate</td>
<td>The Certificate Repository provides a capability to check the status of a certificate. This can be done as part of the &quot;Provide Certificate&quot; function (i.e. the status of the certificate is contained in the certificate when it is delivered) or as a separate function (i.e., returns a simple status flag rather than the entire certificate).</td>
</tr>
</tbody>
</table>

1.3.7 PKI Security Officers

To ensure the Root CA and Subordinate CAs’ 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 CAs, 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).

1.3.8 PKI Registration Officers

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

1.3.9 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 Portima Security Policy (1.3.6.1.4.1.10438.1.1) and Portima Certification Practice Statement (1.3.6.1.4.1.10438.1.2).

1.3.10 PKI System Administrators

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

- Installation, configuration, maintenance and, if necessary, recovery of the OCSP server
- Installation, configuration and maintenance of the certificate management database

1.3.11 PKI System Operators

PKI systems operators are responsible for operating PortiSign trustworthy systems on a day-to-day basis, such as

- Backup and restoration of the certificate management database
- Backup and restoration of PortiSign related servers
1.3.12 **PKI System Auditors**

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

1.3.13 **PKI Secret Holders**

In PortiSign PKI, there are 5 secret holders (cf. Key Ceremony Script).

1.4 **Certificate Usage**

1.4.1 **Appropriate Certificate Use**

The certificate usages for PortiSign Root CA are:
- To generate a self-signed root CA certificate
- To issue and sign the certificates of the subordinate CAs
- To sign the CRL of revoked subordinate CAs certificates

The certificate usages for PortiSign Users CA 10 for qualified certificates and PortiSign Users CA 11 for qualified certificates are:
- To issue and sign the certificates of Subjects
- To sign the CRL of revoked Subjects’ certificates

The certificate usage for Subjects is the digital signature for non-repudiation of documents within the applications operated by Portima.

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 not having agreed with General Terms and Conditions of PortiSign On Mobile;
- By Relying Parties conducting transactions having no relationship to the services and/or applications provided by PortiSign on Mobile.

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 COMDIR for review and approval.
If a change is determined by Portima to have a material impact on the Subscribers or on the Subjects, 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 COMDIR, the date of the modification is updated and the version number is incremented.

A bit OID will be added when version number of the CP will be 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. MyBroker app on mobile is considered as an “Application”.

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 CAs.

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 Certification Authority employs in issuing and managing certificates.
| **COMDIR** | Portima COMDIR 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. |
| **OCSP** | Online Certificate Status Protocol |
| **Personal Identification Number (PIN)** | A PIN having a pre-determined length of five (5) numeric characters is used to protect access to the Subject’s digital signature private keys. PIN protection mechanism is designed in such a way that brute force attacks would result in the destruction of the related private keys. |
| **Portima 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. For instance, insurance brokers subscribing to PortiSign services can act as delegated RAs. |
| **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. BRIO4YOU 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. The Relying Party can be the Subject, a Subscriber, another natural person, a legal entity, CAs, RAs, a software application, or an application server. They rely on certificates for digital signature verification. |
| **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. |
| **Secure Key Box (SKB)** | The SKB is a library that provides cryptographic algorithms. An application that is integrated with |
SKB executes the cryptographic algorithms via the SKB API.

**Subject**

A Subject is a natural person lawfully capable and being older than 18 years old when requesting the service and who uses X.509v3 certificates to electronically sign a document in an Application. Customers of brokers or customers of insurance companies can be Subjects.

**Subscriber**

Subscribers are the brokers who have subscribed PortiSign-related services with Portima. Subscribers act as delegated RA.
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 such as eID picture and mobile number, in an appropriate format to respect privacy
- A repository containing the certificates and CRLs (Certificate Management database)

### 2.2 Publication of Certificate Information

PortiSign documents and information are available 24 hours a day, 7 days per week at [https://www.portisign.be](https://www.portisign.be)

- Any entity using Portima Applications will be provided with the Root CA and sub CA public certificates and the hash of the CA’s public key embedded in the application.
- The root CA and sub CAs certificates are also published at [https://www.portisign.be](https://www.portisign.be)
- Subjects’ certificates are published in a Certificate Management database immediately after issuance.
- When revoked, Subjects’ certificates are published in the CRL (available 24 hours a day, 7 days per week):
  
- The certificate status information is also available via OCSP (available 24 hours a day, 7 days per week):
  

### 2.3 Time and Frequency of Publication
2.3.1 Root CA

See section 2.3.1 of “PortiSign™ Policies and Statements - Users CA 10 and Users CA 11 - Qualified Certificates - Certification Practice Statement”

2.3.2 Subordinate CA

Once created, Subjects’ certificates are published immediately to the repository. Once revoked, a certificate cannot be used for signing anymore. CRLs are published to the repository less than 8 hours after being issued or at least, once a day.

2.4 Access control on published information

This CP is publically available at https://www.portisign.be. The CRL repository is accessible to any end-users (delegated RA, Subjects, Subscribers, relying parties) to enable verification of the certificates.
3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Type of names
The Root CA and Subordinate CAs use an X.500 Distinguished Name format for X500 Subject and Issuer names. Please refer to the Certification Practice Statements “PortiSign ™ Policies and Statements - Users CA 10 and Users CA 11 - Qualified Certificates - Certification Practice Statement” §7.1 for more details.

3.1.2 Uniqueness of names
The set of names in accordance with this CP will be unique within the set of all X500 Subject names in this PKI.
The commonName (CN), givenName (GN) and surname (SN) are based on information extracted from the eID data capture during the face-to-face (first name(s), last name and birthdate).
The X500 Subject contains a serialNumber (SERIALNUMBER) attribute containing a random, unique identifier, and a reference to the Subject’s Delegated RA.
The email address stored in a Subject Alternative Name (SAN) is the email address used by the Subject to log in to the Application.

Please refer to the Certification Practice Statements “PortiSign ™ Policies and Statements - Users CA 10 and Users CA 11 - Qualified Certificates - Certification Practice Statement” §7.1 for more details.

3.1.3 Recognition, authentication and role of trademarks
The RA authenticates the names of the Subjects within this PKI name space.

3.2 Initial Identity Validation
The identity of the Subject is verified and pre-validated by the delegated RA (broker) in a face-to-face meeting. During that meeting, the delegated RA (broker) inserts the Subject’s eID into the smart card reader and, after automated verification by the RA of PortiSign PKI, the eID is saved in the RA management system.

3.2.1 Method to prove possession of private key
Key pairs are generated under the sole control of the Subject on his mobile device.
The Subject proves the possession of his private key by signing the corresponding certificate request.

3.2.2 Authentication of organization identity
N/A.

3.2.3 Authentication of individual identity
The Subject is authenticated to the Application with userID and password.
An SMS with an activation code is sent to the Subject’s mobile number stored in the RA Management System. This code is used on the Subject’s mobile device to start the process.
The Subject takes a picture of his eID with his mobile device and the system extracts identity data from that picture. This identity data is compared by the RA with the eID information already stored in the RA Management System for completing the authentication of the Subject.
3.2.4 Non verified subscriber information
N/A

3.2.5 Validation of Authority
N/A.

3.2.6 Criteria for interoperation
Delegated RA are authenticated to the RA Management System using their certificates issued by the trusted PKI managed by Portima following the CP named Portima Certificate Policy with OID 1.3.6.1.4.1.10438.1.1

3.3 Identification and Authentication for re-key requests
N/A because there is no re-key, Subjects have to request the issuance of a new certificate.

3.4 Identification and Authentication for revocation requests
The identification and authentication for a revocation request is based on a Certificate Revocation Request submitted by either the delegated RA or the Subject.
4. **CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**

For detailed information regarding certificate life-cycle procedures, please see PortiSign™ Policies and Statements - Users CA 10 and Users CA 11 - Qualified Certificates - Certification Practice Statement”, with policy identifier 1.3.6.1.4.1.10438.3.2.4.10.2.

4.1 **Subjects**

Subjects have to meet face-to-face with their delegated RA. The validation of identity required for certificate application is based on information from the Subject’s eID (Belgian citizen card, or type E, E+, F, F+). A Subject is the Subjectholder of a certificate. For details on identification and authentication of Subjects, see section 3.

4.2 **Key pair and certificate usage**

See section 1.4

4.3 **Certificate renewal**

N/A because there is no certificate renewal under this CP and related CPS. Whenever a certificate expires, the Subject is required to generate a new key pair and request a new certificate in accordance with this CP.

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.

4.6 **Certificate revocation and suspension**

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

The Subjects can submit a Certificate Revocation Request from the Application or from the PortiSign portal (https://www.portisign.be), after authenticating with their credentials they are using for authenticating to the Application. The Subjects can alternatively download a document from the PortiSign portal (https://www.portisign.be). The Subjects must print, manually fill and sign the form, and then send the document to Portima with a copy of their eID card. Each time a Subject’s certificate is revoked, the Subject is notified by email and the CRL is issued immediately.

4.7 **Certificate status service**

See section 2.2

4.8 **End of Subscription**

N/A

4.9 **Key escrow and key recovery**

N/A
5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

For detailed information regarding facility, management and operational controls, please see PortiSign™ Policies and Statements - Users CA 10 and Users CA 11 - Qualified Certificates - Certification Practice Statement”, with policy identifier 1.3.6.1.4.1.10438.3.2.4.10.2.

6. TECHNICAL SECURITY CONTROLS

For detailed information regarding technical security controls, please see PortiSign™ Policies and Statements - Users CA 10 and Users CA 11 - Qualified Certificates - Certification Practice Statement”, with policy identifier 1.3.6.1.4.1.10438.3.2.4.10.2.
7. CERTIFICATE, CRL AND OCSP PROFILES

For detailed information regarding Subject's certificate, OCSP’s certificate and CRL profiles, please see PortiSign™ Policies and Statements - Users CA 10 and Users CA 11 - Qualified Certificates - Certification Practice Statement”, with policy identifier 1.3.6.1.4.1.10438.3.2.4.10.2.
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency and circumstances of assessment
Services of these CAs will be audited every 24 months by a conformity assessment body, or upon special request by a conformity assessment body, as laid down in REGULATION (EU) No 910/2014.
Besides this, services of these CAs can be audited by an independent external auditor, upon request of Portima’s shareholders or Insurance Control Bodies or Portima COMDIR.

8.2 Identity/qualifications of assessor
For compliance audits with the REGULATION (EU) No 910/2014, an accredited competent independent professional firm that complies with with ETSI EN 319 403, can qualify as an independent external assessor. The assessor must have a successful track of record with the Belgian conformity assessment body regarding compliance with qualified trust service requirements.
For other audits, the assessor must be independent.

8.3 Assessor’s relationship to assessed entity
The relationship between Portima and its assessors is limited to contractual relationship between parties.
For compliance audits with the REGULATION (EU) No 910/2014, compliance with ETSI EN 319 403 is also required.

8.4 Topics covered by assessment
The purpose of the audit shall be to confirm that Portima and the PortiSign on Mobile qualified trust service fulfil the requirements laid down in REGULATION (EU) No 910/2014.
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 risk or risks involved.

8.6 Communication of results
Besides exceptions required for reporting to the Belgian conformity assessment body, for security reasons, the audit results are not published or provided to parties external to Portima.
For non REGULATION (EU) No 910/2014-related audits, Portima retains the right to refuse to publish any audit results for security reasons. However, audit results will be communicated to Relying party representatives on a case-by-case basis.
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
Please refer to General Terms and Conditions for PortiSign on Mobile.

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.
• PKI Contingency and Business Continuity plans.
• Subjects’ private key and 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 can’t contain confidential information or privacy sensitive information.

9.3.3 Responsibility to protect confidential information
Entities allowed to access confidential information can’t 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:

- 7 years (2 years for certificate validity window + 5 years)
- The duration required by the business requirements related to the signed documents.

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 Terms and Conditions for PortiSign on Mobile. Other liability issues are dealt with in contracts between relevant parties.

9.8 Indemnities
Please refer to General Terms and Conditions for PortiSign on Mobile.

9.9 Term and Termination
If Portima ceases its PKI activity, it will keep providing information allowing the verification of digital signatures for 10 years. A PortiSign Termination plan (OID 1.3.6.1.4.1.10438.3.1.5) is set up; it defines the termination processes that must be executed to properly shut down the PortiSign PKI activity related to the issuance of qualified certificates.
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 COMDIR for review and approval. During this ad-hoc meeting, PKI Security Officers inform members of Portima COMDIR of intended changes, their impact on the existing CP, and his recommended actions. A decision is taken by Portima COMDIR 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 his delegated RA (broker), which will endeavour promptly to resolve the dispute or escalate to Portima.

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 9.4

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
Aside from legal requirements restricting the usage of signature, PortiSign 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.