Portima
Certificate Policy

Version 1.0

http://www.port-e-key.be
http://vpn.port-e-key.be
E-mail : help@port-e-key.be
Call center : +32 (0)2 404 44 22
Fax : +32 (0)2 404 44 49

TABLE OF CONTENTS

1. TERMINOLOGY

Access Control Database (ACD)
The Access Control Database is a repository that contains a Subscriber's privileges.

Business Partner
A business partner is considered a Company or Broker who have entered into a contractual agreement with Portima for the purposes of sending, receiving, and storing data on Portima's network infrastructure.

Certificate
The certificate is a digital object that binds a Subscriber's name to a public key or keys. 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.

For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions.

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 unexpired certificates that should not be trusted. 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 the people who operate it. The CA performs four basic operations:

- Issues certificates (i.e., creates and signs them) for the Registration Authorities, Local Registration Authorities, End Users, and Entities.
- Maintains certificate status information and issues CRLs
- Publishes certificates and CRLs
- Maintains archives of status information about expired or revokes certificates that it issued.
- Portima owns and operates the Root and subordinate CAs.

Certification Path
An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

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

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 Directory where the certificate is held.
Entity	An Entity within the Portima PKI is a non-physical person such as an Application or Application Server.
External Party	Entities engaged in B2B transactions with Portima but outside the Insurance Company and Broker sphere.
Issuer	Portima who owns and operates the CA acts as issuer of public key certificates.
Local Registration Authority (LRA)	The LRA is designated to verify certificate contents for the CA at the Broker, Company, or External Party premises. The RA collects and verifies information for the User before a request for a certificate is submitted to the CA.
Portima Software Certification Officer **(PSCO)**	The PSCO is designated by Portima to verify signature integrity and origin of software provided by Software Project Leaders, when this software has to be distributed or used by Portima.
PIN	A Personal Identification Number having a pre-determined length of eight alphanumeric characters used to protect access to the Subscriber's or Entity's encipherment and digital signature private keys.
Policy Approval Committee	The Portima Policy Approval Committee (PAC) determines the suitability of a CPS and its compliance with the CP(s).
Portima	Owner and operator of the CA and RA.
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 is a collection of computer hardware, software, and the physical persons who operate it. The RA's principle role is to bind the subject of a certificate to his private key pair. The RA performs this role through the application, verification, and registration processes involved when requesting a certificate for the Subscriber or Entity.
Relying Party	Relying parties use the PKI to implement security services by employing the public key in another user's certificate. They can verify digital signatures, encrypt data and use the public key in another party's certificate to establish a symmetric key through key agreement. Relying parties may include CAs, RAs, persons, and computing systems such as routers and firewalls. A relying party interacts with the repositories on a day-to-day basis.

	Its interaction with CAs is limited to selection of an initial trust point.
Repository	A repository accepts certificates and CRLs from one or more CAs and makes them available to parties that need them to implement security services. The Repository means the Directory.
Software Project Leader (SPL)	SPL certifies the origin and the absence of malicious behaviour of code that should be distributed to other parties. If this code has to be distributed by Portima, code has to be counter-signed by a PSCO.
Subscriber	Subscribers obtain certificates from the infrastructure and use their private keys to implement security services. They generate digital signatures, decrypt data, and use their private key agreement between themselves and users. A Broker's, Company's, and External Party's LRA and Users are considered Subscribers within the Portima PKI. Portima's RA and Users are also considered Subscribers within the Portima PKI.
Third Party	Third parties are those organizations not directly affiliated with Portima but have a business relationship with Companies who participate in the Portima PKI.

2. OVERVIEW

The Portima Public Key Infrastructure service provides security and trust for electronic transactions through Portima.

The Portima Port-e-Key Certificate Policy (hereinafter referred to as "CP") is a statement regarding the policies that the Portima Certification Authority (CA) 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 2527) dated 12 July 2001. However, the table of contents set out in this RFC has been modified in order to meet the needs of the Portima Port-e-Key PKI.

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

2.1 Identification

This CP is called "Portima Port-e-Key Certificate Policy, Version 1.0". The Policy ID for this CP is as follows:

Policy ID
xxxx

2.2 Applicability

Certificates that are issued under this CP will be used for the following functions:

- Authentication of Subscribers and Entities;
- information integrity;
- confidentiality;
- access control; and
- non-repudiation.

The table below lists the entity and applicability of the certificates issued by the CA:

Entity	Certificate Usage	CRL Signing	Certificate Issuing	End-user operations Authentication, confidentiality, integrity, non-repudiation[1]	Application security	Application Server security	CA Operations	Code Signing
Root CA	To generate digital signatures for signing Subordinate CA certificates and Certificate Revocation Lists.	x	x					
	To generate a self-signed root CA certificate.		x					
Subordinate CA	To generate digital signatures for signing Subscriber certificates, and Certificate Revocation Lists.	x	x					
Registration Authorities (Portima Ras and LRAs)	To authenticate the RA to the Certification Authority, Application Server,or Application			x	x	x		
	To *encrypt* data transported over Portima's network from a Subscriber's workstation to an Application Server or Application.			x	x	x		
	To generate digital signatures for non-repudiation of data communicated over Portima's network.			x	x	x		
Portima Security Officer	To authenticate the SO to the Certification Authority, Administrator Workbench, Key Generation System, Certificate Controller, and other systems that interact with the Certification Authority.						x	
Portima Software Certification Officer	To generate digital signatures for code signing for software applications distributed by Portima.							x

Subscriber (including SPL)	To *authenticate* the Subscriber to an Application Server or Application operated by a Business Partner or Portima.			x	x	x		
	To *encrypt* data transported over Portima's network from a Subscriber's workstation to an Application Server or Application.			x	x	x		
	To generate digital signatures for non-repudiation of data communicated over Portima's network.			x	x	x		
	Encryption of a session key generated by the User's browser or other proprietary software package in order to guarantee its confidentiality when transmitted to the Application Server or Application processes.			x	x	x		
	To generate digital signatures for code signing of software applications to be distributed directly or by Portima.							x
Relying Party	To *authenticate* the Application Server or Application to a Subscriber .			x	x	x		
	To *encrypt* data transported over Portima's network from the Application Server or Application to another Application Server or Application or Subscriber.			x	x	x		
	To generate *digital signatures* for non-repudiation of data.			x	x	x		

2.2.1 Restricted use

Certificates and CRLs issued under this CP will only be used by Users and Application Servers made available through and by Portima. Certificates issued under this CP will not be used in communications with parties other than Portima.

Digital certificates issued by the Portima PKI may not be used:

- By Applications other than those described in **Error! Reference source not found.**;

- By third party Subscribers or Relying Parties with no contractual relationship with Portima's Business Partners or without a Business Partners obtaining prior agreement from Portima.

- By Subscribers or Portima employees conducting transactions having no relationship to the services and/or applications provided by Portima;

- By Subscribers or Portima employees for personal secure email.

2.3 Community

2.3.1 Issuer

Portima acts as the certificate issuer. The issuer fulfills the roles of:

- Certification Authority;
- Registration Authority (RA); and
- Repository.

2.3.2 Certification Authorities

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

The Portima PKI is comprised of the following CAs:

- Portima PKI Root CA (herein referred to as "Root CA");
- Port-e-Key Portima PKI Community CA (herein referred to as "Subordinate CA").

2.3.3 Registration Authorities

The Subordinate CA delegates tasks, as described in Section 0, 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 (herein referred to as "LRA")

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 LRA. 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).

To facilitate the certificate enrolment process, the PRA delegates tasks such as certificate application, identity validation, and certificate authorization to a Business Partner's LRA. These local 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.

2.4 Security Officers

To ensure the Root and Subordinate CA's integrity and security, Portima employs a Security Officer (herein referred to as "SO"). The SO's principle role is the security of the CAs. In addition, they manage the day-to-day operations of the Subordinate CA, revoke RA, LRA, Subscriber, and Entity certificates in accordance with this CPS.

2.5 Subscribers and Entities

The PKI considers a Subscriber as a natural person who use 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.

The Portima 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. These application may reside at a Business Partner's, or Portima's premises.

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. These application servers may reside at a Business Partner's, or Portima's premises.

2.5.1 Relying Parties

This CPS defines a Relying Party as a recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. The Relying Part can be a natural person, software application, or application server.

A Relying Party may be an Subscriber or Entity. They rely on certificates for authentication, decryption, and digital signature verification.

2.6 Contact Details

All questions and comments concerning the this CPS should be addressed to:

Christophe Cloesen
Portima Security Officer
Chaussée de la Hulpe 150
1170 Bruxelles
Belgium

Tel: +32 (0)2 661 44 11
Fax: +32 (0)2 661 44 49
Email: security@portima.com

3. GENERAL PROVISIONS

3.1 Subscribers' obligations

3.1.1 Applications

Subscribers obtaining certificates are responsible for the proper use of the certificates and private keys. The form of acceptance of a certificate can be found at §0 in this CP.

3.1.2 Protection and use of private keys

After a Subscriber accepts its certificates, they must protect the private keys issued to it. They must ensure that the keys are accessible only to designated authorized persons, and that the private keys and the associated PIN codes are not stored together. They must immediately report any unauthorized use or loss of the private keys to the RA. A private key must not be duplicated, copied or backed up.

Upon suspension or revocation of their certificates, they must cease using their private keys.

3.1.3 Protection of certificates

3.2 Disputes

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

3.3 Amendment of CP

Portima may amend this CP at any time by giving not less than 10 business days prior written notice to Subscribers. No amendment will have retrospective effect.

3.4 Publication and Repositories

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. This section should be read together with §10 of this CP.

3.4.1 Publication of Portima CA information

Brokers, Companies, and External Partys using the PKI will be provided with the CA public certificate and the hash of the CA.

3.4.2 Access control on published information

This CP will be available to all Subscribers who use Portima. The certificate directory and CRL will be accessible to the RA, LRA, Users to enable browsing of all certificates and CRLs.

3.4.3 Use of Repositories and CRLs

Portima will use the Repository and CRLs in order to check digital signatures. Subscribers and Entities will check the repository to verify public certificates and to check CRLs.

3.5 Fees

3.5.1 Certificate issuance or renewal fees

Obtainable from Portima

3.5.2 Certificate access fees

Obtainable from Portima

3.5.3 Revocation or status information access fees

Obtainable from Portima LRAs

3.5.4 Fees for other services such as policy information

Obtainable from Portima LRAs

3.5.5 Refund policy

Obtainable from Portima LRAs

3.6 Compliance audit

3.6.1 Frequency of entity compliance audit

Services of the CA will be audited on an annual basis by an independent external auditor.

3.6.2 Identity/qualifications of auditor

The independent external auditor will be employed by a competent independent professional firm that complies with appropriate national and international standards and codes of practice.

3.6.3 Auditor's relationship to audited party

Limited to contractual relationship

3.6.4 Topics covered by audit

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

3.6.5 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.

3.7 Confidentiality

3.7.1 Disclosure of information relating to certificate revocation

Only the Subscriber who accepted the certificate will be informed of the reason for revocation of that certificate.

3.7.2 Correction of certificate data

To correct certificate data, the Subscriber's LRA or Department Head must revoke the certificate following the procedures described in the CPS and request a new certificate with the corrected data.

3.8 Ownership of CP

This CP is the absolute property of Portima and must not be copied, modified or reproduced without Portima's prior written consent.

This CP may be stored on disk, tape or other electronic device provided the medium of storage is not accessible to anyone except the Subscriber.

3.9 Intellectual Property Rights

No right or interest in any intellectual property rights are granted to the Subscriber or Relying Party under this Certificate Policy. All rights in intellectual property are reserved to the CA or the RA as set out in the contract between them.

4. INITIAL REGISTRATION

4.1 Types of names

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

Entity	Attribute	Description
PRA and PSO	Name	Full name of the LRA 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 LRA
	UserID	Unique UserID
	Office ID	Broker's unique Office ID
Subscribers	Name	Full name of the LRA 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 LRA
	UserID	Unique UserID
	Office ID	Broker's unique Office ID
Application Server	Master Server	Application Server name
	Master Service	Application Server Service
	IP Address	Application Server's IP address
	IP Port	Application Server's IP Port

4.2 Uniqueness of names

The set of names in accordance with this CP will be unique within the set of all Subscriber names in the Portima PKI as follows:

cn = <user>, ou = < >, ou = < >, ou = <companies>

4.3 Name claim dispute resolution procedure

The names used in the certificate are names that are attributed and used only by Portima.

4.4 Recognition, authentication and role of trademarks

The PRA authenticates the names of an LRA, Users, Application Servers, and Applications within the Portima name space. An LRA authenticates the names of his Subscribers and Entities within the Portima name space.

4.5 Method to prove possession of private key

The CA ensures, by verification of the signature, that the Subscriber demonstrates the possession of the secret signing key by signing a piece of unpredictable data supplied as part of the application process.

4.6 Authentication of organization identity

Any existing contract between Portima and the business partner will constitute authentication of the Subscriber.

4.7 Authentication of individual identity

The following tables describes authentication of individual identity including entities within the Portima Port-e-Key PKI.

Validation of Identity	Method
LRA	Face-to-face registration with the PRA at which time the LRA's identity is verified against a national identity card.
Subscriber	Business Partner's LRA validates the identity of a Subscriber. For code signing certificates, the Software Project Leader and Portima Software Certification Officer register in-person with the PSO.
Entity	Business Partner's LRA 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 names and/or IP address.

5. KEY PAIR MANAGEMENT

5.1 Key pair generation and installation

Input to the key pair generation process will be a random number, created in such a way and being of such length as to make it computationally impossible to regenerate it, even with knowledge of the time when, and the equipment on which, it was generated.

The generation procedure and storage of the private key prevent it from being exposed outside the system that created it.

Subscriber and Entity key pairs are locally generated during the requesting process or by the CA during the enrollment procedure. Keys may be generated in hardware or software as long as they meet the requirements in this CP. The following table describes the method used to generate key pairs for each type of certificate.

Certificate type	Method	No. of certificates	Hardware/Software
Certificate Authority	Hardware Security Module (HSM)	1	Hardware
PRA, PSO	Smart card	2	Hardware
Subscriber and Entity certificates	Browser or application	2	Software
Subscriber and Entity (smart card)	Application	2	Hardware

5.2 Private key delivery

The Portima Port-e-Key PKI issues soft certificates (browser) and smart card based certificates. For soft certificates Subscribers and Entities generate the private key(s) on their workstations or application servers.

The smart card containing the private key, protected with its initial activation PIN code, will be distributed to the Subscriber in a way that prevents it from being found together with the activation PIN code, until it has been delivered to the user. The private key pairs do not leave the smart card.

5.3 Private key lengths

The following key lengths are used in the Portima PKI.

Entity	Key length
Root and Subordinate CAs	2048 RSA
PRA, PSO, Subscribers, and Entities	1024 RSA

5.4 Private key usage

The key usage extension in X.509v3 certificates defines the purpose (e.g., encipherment, digital signature, and non-repudiation) of the key contained in the certificate.

5.5 Private key protection

The Portima Security Officer will verify that the private keys of the PRA and the corresponding means of their usage are protected by, and restricted to, a smart card that has been delivered to the PRA.

The LRA will verify that the private keys of his subscribers and Entities and the corresponding means of their usage are protected by, and restricted to, a single computer system.

5.6 Standards for the cryptographic module

A CAs' private issuing keys used for signing certificates and related objects such as CRLs and CA certificates will be protected by high assurance physical and logical security controls. The keys are contained and operated from inside a FIPS 140-1 level 3-compliant hardware Security Module (HSM). Any unauthorized attempt to gain access to the HSM will destroy the key. A split-knowledge technique (n of m) ensures that a cryptographic key is under the control of more than one person. Each person has a key component, which, individually, provides no details of the resultant key.

5.7 Private key (n of m) multi-person control

The private key of a PRA, PSO, Subscribers or Entities will not be under (n out of m) multi-person control.

Dual control is required to access or use the CAs' private certification keys for any purpose.

5.8 Private key recovery

[To be completed.]

5.9 Private key activation

5.9.1 Smart card certificate

Each call to the algorithmic function will require that the smart card have been activated with a correct PIN code. The same PIN code controls the use of all private keys in the smart card.

A smart card will block itself after three consecutive failed attempts at giving the PIN code. Unblocking a blocked smart card requires the Subscriber to enter the correct Pin Unblocking Code (PUC). A PUC will only be delivered to the registered Subscriber or Entity along with the PIN code.

The Subscriber or Entity's private key will be protected from exposure and unauthorized use by a PIN code.

5.9.2 Soft certificate

Subscribers and Entities who use soft certificates must activate their private keys with the correct PIN code. Soft certificates do not employ a PUC.

5.10 Other aspects of key management

5.10.1 Usage periods for the public and private keys

The following table shows the validity period for public and private keys.

Entity	**Validity**
Root CA	20 years
Subordinate CA	10 years
PRA (including LRA)	3 years
Subscriber and Entity	1 year or 3 years

Each CA will state, in the certificate, a restricted validity period for the certificate itself. During the certificate validity period each CA will provide adequate revocation services.

5.10.2 Activation data

A PIN code protecting the usage of private keys and the PUC in smart cards will consist of at least eight (8) alphanumeric characters. The RA will be forced to change the PIN code on first log on.

A PIN code protecting the usage of private keys for browser and Application Server certificates will consist of no less than eight (8) alphanumeric characters. The User will be forced to enter a PIN code during the private key generation process.

6. CERTIFICATION

For detailed information regarding the certification policy and procedures for Subscribers and Entities, please see the "Portima Certification Practice Statement version 1.0", section §4 Certificate Life-cycle Operational Requirements.

6.1 Certificate acceptance

For detailed information regarding the certification acceptance policy and procedures for Subscribers and Entities, please see the "Portima Certification Practice Statement version 1.0", section §4 Certificate Life-cycle Operational Requirements.

6.2 Certificate renewal

For detailed information regarding certificate renewal policy and procedures for Subscribers and Entities, please see the "Portima Certification Practice Statement version 1.0", section §4.7 Certificate renewal.

6.3 Routine re-key

For detailed information regarding the routine re-key policy and procedures for Subscribers and Entities, please see the "Portima Certification Practice Statement version 1.0", section §4.6 Key changeover.

6.4 Certificate Suspension

Portima may suspend the functional privileges of a Subscriber or Entity upon request of the Portima Security Officer or the Subscriber. An LRA may suspend the functional privileges of a User, Contractor and temporary employee.

6.4.1 Status checking requirements

User related data contained in the ACD is the responsibility of the owner of the application(s).

To maintain currency, Portima and the business partner must periodically cross-check the list of authorized Users against staff lists and roles, and prepare in advance for the revocation of changing of a User's access rights to coincide with their leaving the organization or changing roles.

6.5 Certificate Revocation

6.5.1 Circumstances for revocation

Permissive Revocation

A Subscriber may request revocation of a certificate at any time for any reason. An Issuing CA 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.

Required Revocation

A Subscriber will promptly request revocation of a certificate:

- 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 Subscriber is no longer affiliated with a business partner's organization.

For the purposes of this section, Portima will revoke a Certificate:

- Upon request of the Subscriber or business partner;
- Upon failure of the Subscriber to meet its material obligations under the CP, this 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
- If there are any other grounds for revocation.

6.5.2 CRL issuance frequency

Portima publishes its CRL once every hour. The validity of a CRL is 24 hours.

6.6 Revocation requests

For detailed information regarding certificate revocation and suspension procedures for Subscribers and Entities, please see the "Portima Certification Practice Statement version 1.0", section §4.10 Certificate Revocation and Suspension.

6.7 Revoked CA public key

In the unlikely event that a CA private key is revoked, the certificates for the entire Subscriber community must be re-issued in accordance with the following procedure:

- The issue notifies the entire subscriber community of the CA re-certification;
- The CA generates a new CA key pair and certificate;

- The PRA performs a setup for recovery of all LRAs or Users and securely distributes new PINs;
- The LRAs then performs setups for recovery of all Users belonging to their area of control and request new certificates.

6.8 Compromise and disaster recovery

This section describes requirements relating to notification and recovery procedures in the event of compromise or disaster.

6.8.1 Recovery in case of corruption

In case of loss of integrity or suspected loss of integrity of computing resources Portima will take, as appropriate, one or more of the following actions:

- Should the primary site's computing resources loose integrity, Portima will take the site offline. The secondary site automatically becomes the primary site whilst the primary site is rebuilt from available back-up or a clean install;
- Should both the primary and secondary sites' computing resources loose integrity, Portima will take the system temporarily off-line and re-open it when one of the two sites becomes fully operational. Portima will notify all Subscribers, via their LRAs, of the situation. LRAs will be requested to inform their respective Users. Portima will provide an estimate of when it expects the system to become fully operational again;
- Portima will perform integrity checks before commencing to rebuild the system;
- Portima will safeguard against any uncontrolled access to PKI components during this time.

6.8.2 Recovery after compromise

In case of compromise of any part of the system, the following steps will be taken:

- That part of or the whole system is taken off-line depending on the situation.
- The related keys are immediately revoked.
- Portima notifies all PRAs, via the Security Officer, and all Subscribers, via their LRA, of the change and its reasons via e-mail and telephone. Subscribers will be requested to inform, and responsible for informing their Users. Portima will state whether its services are still to be trusted, when it expects it will become fully operational again.
- The system is then completely reinstalled based on available backups and/or clean components (as the situation requires)
- A re-key of the system is performed
- When the system goes on-line again, the participants will be similarly informed.

6.8.3 Recovery after disaster

After any disaster:

- The backup site takes over while the primary site is being rebuild based on available backups and/or clean components (depending on the situation).
- The equipment and software at the site affected will be guarded against any thefts or uncontrolled removal.

- The disaster is likely to be transparent to Subscribers unless both sites are affected by a disaster, after which the system will go off-line to be rebuilt completely.
- If the Portima system needs to go off-line, Portima will at that time notify all internal staff (via Portima's Security Officer) and all Subscribers (via their LRA) of the fact and the reasons for it via e-mail and telephone. The Subscribers will be requested to inform, and be responsible for informing, their Users. Portima will state when it expects to become fully operational again. When the Portima system goes on-line again, the Subscribers will be similarly informed.

6.9 CA Termination

Termination of a CA occurs when all services associated with a CA are terminated permanently. Termination does not occur where the service is transferred from one organization to another or where the CA service is passed over from an old CA key to a new CA key.

In order for the CA to terminate its services, the following procedures must be completed:

- The CA will inform all Subscribers with which the CA has agreements
- Give public notice of its termination at least three months prior to termination
- Terminate the revocation checking service for all certificates issued under the terminated issuing keys. This will stop any of these certificates from being accepted by any party who follows proper revocation-checking procedures.

The CA will maintain the archives for ten (10) years from creation date.

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate profile

7.1.1 Version number

Certificates issued under this CP will be constructed according to ISO 9594-8 (X.509). The version will be version v3.

7.1.2 Certificate extensions populated and their criticality

Following standard extensions are used for CA, smart card, and browser certificates:

Certificate type	Extension	Criticality	Meaning (RFC2459)	Value
CA	Basic constraints	Critical	Identifies whether the subject of the certificate is a CA and how deep a certification path may exist through the CA.	cA= TRUE
	Authority Key Identifier	Non-critical	Identifies what public key corresponding to the private key is used to sign a certificate.	One of the keys as defined by this CP.
Smart card	Key usage	Critical	The purpose of the key contained in the certificate.	nonRepudiation (1) or; digitalSignature (0) and keyEnciphermen t (2)
	Subject alternate name	Non-critical	Additional identities to be bound to the subject of the certificate.	E-mail address of the certificate holder.

It is also recommended the use of other two extensions: CRLDistributionPoint for providing information useful to retrieve the CRL. This extension should be marked as NOT CRITICAL.

No private extensions will be used.

7.1.3 Cryptographic algorithm object identifiers

Certificates issued under this CP will use the following OIDs for signatures:

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

7.1.4 Name forms used for the CA, RA, Subscriber and Entity names

See §4.1 of this CP.

7.1.5 Name constraints used and the name forms used in the name constraints

See §4.2 of this CP.

7.2 CRL profile

The Portima CRL-environment is according to X.509 version2 (excluding CRL extensions).

8. PHYSICAL AND OPERATIONAL REQUIREMENTS

8.1 Physical Controls

The infrastructure for the majority of PKI components resides in the secure production area at Portima's premises. Network connections to and from these components are protected through encryption.

Physical access to these hardware components, networks and information will be restricted to designated employees on a need to know basis. Access to PKI components requires the presence of at least two persons.

The environments where registrations are operationally and administratively processed will be sufficiently protected. The RA will ensure that only authorized employees have access to the location where the administrative processing of confidential Subscriber information is performed.

Portima repositories have a place to store backup and distribution media in any manner sufficient to prevent loss, tempering, or unauthorised use of the stored information. Backups are kept both for data recovery and for the archival of important information.

8.2 Power and air conditioning

The power supply of the server components is protected against a main network power supply interruption. All servers are connected to a no-break system.

Stable temperatures for the PKI hardware equipment are guaranteed by an air conditioning system. This system is installed in such a way that it will not reduce the physical security of the room nor compromise the functioning of the hardware/software.

Internal Portima policy regarding fire prevention and protection is applied.

9. LOGGING AND ARCHIVING

9.1 Logging

Security audit procedures apply to all computer/system components, which affect the certificates issued under this CP.

The Portima Security Officer will aim to keep up-to-date with relevant information security standards and be aware of security related issues to ensure compliance with these procedures.

Audit trails will provide a mechanism for recording and subsequently tracing the actions of individuals. Hence, recorded information will include the identity of the individuals performing any action to access the information and the time the access occurred.

Portima will assess the security and vulnerabilities of their information systems at its premises on an ongoing basis. The Security Officer will analyse the log-files and have the right to add other events to be logged in order to improve security.

Log files will be consolidated and analysed for evidence of malicious behaviour on an ongoing basis.

Audit logs will be retained for a period of ten (10) years.

9.2 Escalation procedure

If the Security Officer obtains evidence of careless or incorrect operations or malicious behaviour, he will start-up the escalation procedure. This procedure will, depending on the action, include actions at three major levels:

- Organizational actions;
- Operational actions;
- Technical actions.

9.3 Records Archival

Portima has implemented systems and processes to ensure the integrity of the data maintained by it in its capacity as Certification Authority. Daily database backups are performed to be able to restore the system to a known baseline. These backups are kept under strict configuration control. Data is periodically removed from the databases and stored off-line in a secure facility. The retention period for archived data is ten (10) years from its date of creation. Access to and archived data is restricted by a control list of screened personnel. Additionally, a functionally identical backup Certification Authority system is maintained to support business resumption.

10. SPECIFICATION ADMINISTRATION

10.1 Items that can change without notification

Changes may be made to this specification without prior notification under exceptional circumstances.

10.2 Items whose change require a new version number

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

10.3 Version administration

10.3.1 All changes

Each time the CP has been modified with the approval of Portima management, the date of the modification will be updated and the serial number will added to the document.

10.3.2 Distribution of the CP

The Portima CP shall be available to all participants who intend to use this environment. This CP can be retrieved in either of the following ways:

- Distribution via CDROM;
- Distribution via publishing on the Portima web site; or
- Distribution via paper document.