PEPPOL
PAN-EUROPEAN PUBLIC PROCUREMENT ONLINE

Guideline

OpenPEPPOL

Pan-European Public Procurement Online

Transport Infrastructure
ICT
Services-Components

Trust Network
Certificate Policy

Version: 2.00
Status: In Use

Editors:
Thomas Gundel, DIGST/IT Crew
Sven Rasmussen, DIGST

Revision History

Version	Date	Editor	Org	Description
1.00	18.07.2011	Thomas Gundel	DIGST	
1.1	09.11.2012	Thomas Gundel	DIGST	Updated to reflect transition to OpenPEPPOL with new PKI setup from Symantec and adjusted enrollment process.
2.00	07.07.2014	Sven Rasmussen	DIGST	Updated references and editorial changes

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Contributors

Organisations

DIGST (Digitaliseringsstyrelsen), DK, http://www.digst.dk/
DIFI (Direktoratet for forvaltning og IKT), NO, http://www.difi.no/

Persons

Thomas Gundel, DIGST/IT Crew
Sven Rasmussen, DIGST
Klaus Vilstrup Pedersen, DIFI

Table of Contents

1 Introduction

1.1 Objective and Scope

PEPPOL (Pan-European Procurement Online) is a project under the EU Commission's CIP programme with the goal of setting up a pan-European solution that facilitates EU-wide interoperable public eProcurement. The vision of the PEPPOL project is that any company and in particular SMEs (Small and Medium Enterprises) in the EU can communicate electronically with any European governmental institution for the entire procurement process.

As the Pan-European Public Procurement Online (PEPPOL) project reached a successful completion on August 31st, 2012, with the PEPPOL specifications being implemented across Europe, the OpenPEPPOL Association has been set up to take responsibility for the maintenance of the OpenPEPPOL specifications, building blocks and services, and to promote implementation across Europe.

OpenPEPPOL has been established as a non-profit international association under Belgian law, comprised of interested public and private members of the OpenPEPPOL community and has begun official operations on September 1st, 2012. Membership is now open to a wide range of organisations.

The Association provides the authoritative point of reference for networks of interoperable, OpenPEPPOL-compliant infrastructure and the organisations that use it, ensuring high-level governance and continuation of the agreement infrastructure.

In the technical infrastructure, supporting OpenPEPPOL a mechanism is needed whereby trust between parties can be enabled. For this purpose OpenPEPPOL is deploying a hierarchy of Certificate Authorities (hereafter called OpenPEPPOL Trust Network or *PTN*). The hierarchy will consist of a OpenPEPPOL root CA with three sub CAs. The OpenPEPPOL root CA will issue certificates for the sub CAs only.

The PTN will provide certificate services for a community of organizations that are service providers of Pan-European Procurement Online and members of the OpenPEPPOL organization. More specifically, the OpenPEPPOL sub CAs will issue digital certificates to organizations running the following OpenPEPPOL infrastructure services: Access Points, Security Token Services and Service Metadata Publishers. Operators of these services are called OpenPEPPOL service providers and can be private companies as well as government institutions.

An organization who wants to become an OpenPEPPOL service provider and obtain an OpenPEPPOL certificate must first enter a legal agreement with a OpenPEPPOL Authority and become a member of the OpenPEPPOL organization. These agreements are the “OpenPEPPOL AP Provider Agreement” [APA] and/or the “OpenPEPPOL SMP Provider Agreement” [SMPA]. There is currently no agreement for OpenPEPPOL Security Token Services.

OpenPEPPOL certificates are used for digital signatures on protocol messages for purposes of authentication and integrity, for client authentication (e.g. SSL / TLS) and may optionally also be used for encryption of messages.

This document, “The OpenPEPPOL Trust Network Certificate Policies” (CP) is the principal statement of policy governing the PTN. The CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing digital Certificates within the PTN. These requirements protect the security and integrity of the PTN and comprise a single set of rules that apply consistently PTN-wide, thereby providing assurances of uniform trust throughout the PTN.

This document is targeted at:

- PTN certificate Subscribers (i.e. OpenPEPPOL service providers) who need to understand how they are enrolled and what their obligations are as PTN subscribers and how they are protected under the PTN.

- Relying parties who need to understand how much trust to place in a PTN certificate, or a digital signature using that certificate.

The CP, however, does not govern any services outside the PTN.

1.2 Audience

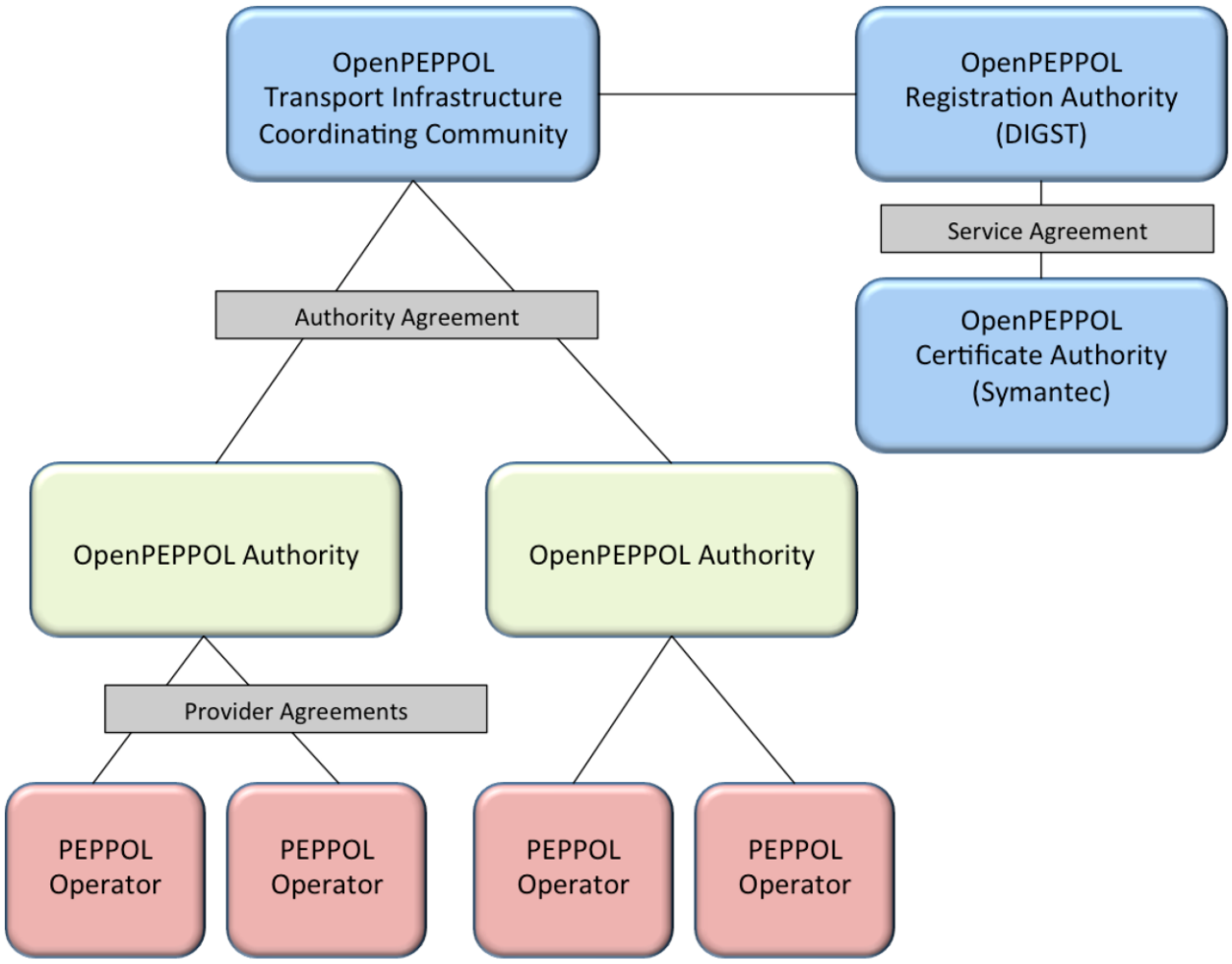
OpenPEPPOL Stakeholders:

- ICT Architects
- ICT Developers
- ICT Governing participants

1.3 Overview

This CP is structured in accordance with RFC 3647 of the Internet Engineering Task Force (IETF) to set out the policies under which PTN participants must operate.

An overview of the OpenPEPPOL governance model for the transport infrastructure is shown in the figure below:



Essentially, OpenPEPPOL transport infrastructure is governed by a two-layer model consisting of a central coordinating authority (Transport Infrastructure Coordinating Community or TICC) responsible for the overall

technical coordination including technical standards, policies, common infrastructure components etc. supplemented by OpenPEPPOL Authorities responsible for implementing the OpenPEPPOL infrastructure within their domain which is typically countries or regions within a country. Please refer to annex 7 of the OpenPEPPOL "Transport Infrastructure Agreements" for details on the governance model [PCA].

As part of the shared, central infrastructure, an OpenPEPPOL Certificate Authority has been established by the Danish Digitisation Agency (DIGST) on behalf of OpenPEPPOL (purchased as a managed service from Symantec). The CA issues the certificates described in this document. Further, DIGST will perform the role of central Registration Authority with the purpose of setting up and managing the CA, and coordinating registration of OpenPEPPOL service providers (operators).

Digital Certificates issued under the PTN shall be used to secure communication within the OpenPEPPOL infrastructure – i.e. by digital signature, authentication or encrypting information.

The organization who ultimately receives a digitally signed document or communication is referred to as a Relying Party, i.e., he/she is relying on the certificate and has to make a decision on whether to trust it.

1.4 Document Name and Identification

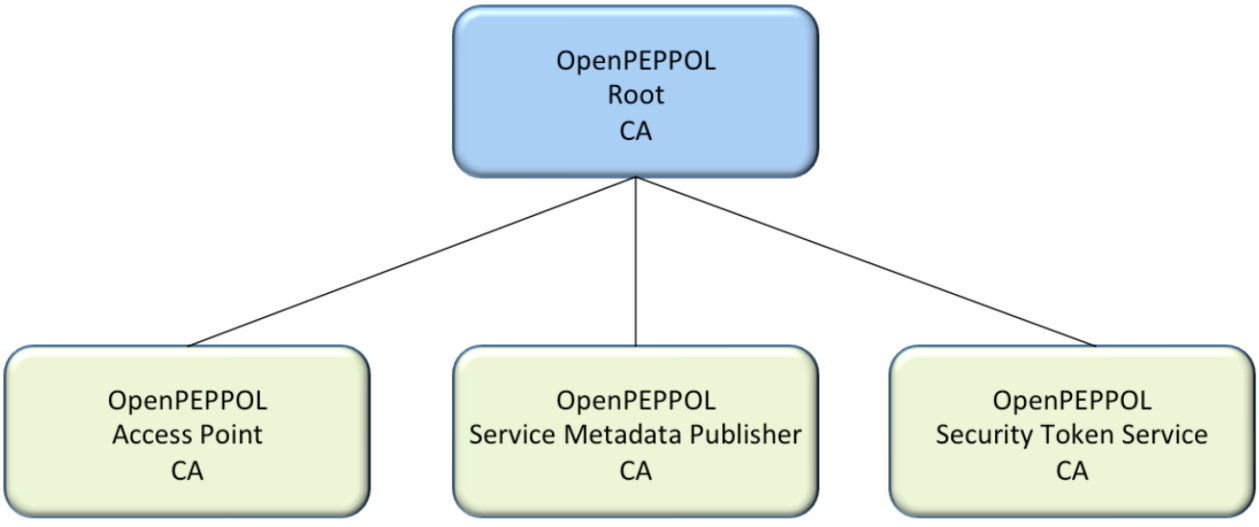
This document is the OpenPEPPOL Trust Network Certificate Policy (CP). OpenPEPPOL, acting as the policy-defining authority, has assigned an object identifier value extension for each type of Certificate issued under the OpenPEPPOL Trust Network (PTN). The object identifier values used for the types of end-user Subscriber Certificates are:

• The OpenPEPPOL Certificate Policy: located at www.Peppol.eu

1.5 PKI Participants

1.5.1 Certification Authorities

The term Certification Authority (CA) is an umbrella term that refers to all entities authorized to issue public key certificates within the PTN. In the PTN, Symantec is operating all Certificate Authorities as a managed service.



PTN will consist of one root CA with three sub CAs issuing each of the three types of OpenPEPPOL certificates:

- OpenPEPPOL Access Point Sub CA
- OpenPEPPOL Security Token Service Sub CA
- OpenPEPPOL Service Metadata Publisher CA

Certificates issued under these three subordinate CAs will generally be referred to as “OpenPEPPOL Certificates” in this document.

1.5.2 Registration Authorities

A Registration Authority (RA) is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of a PTN CA.

In the OpenPEPPOL Trust Network, two entities will perform registration tasks:

- OpenPEPPOL Authorities will handle the identification and authentication of certificate applicants (prospective OpenPEPPOL service providers). This includes entering contractual agreements (Transport Infrastructure Agreements) with these, ensuring that the organization is a member of the OpenPEPPOL organization, and validating their business registration credentials.
- The central OpenPEPPOL Registration Authority will receive approved applications from OpenPEPPOL Authorities, register the applicant with the CA, and create/deliver a passcode for the applicant for subsequent enrollment for OpenPEPPOL Certificates.

In order to become a OpenPEPPOL Authority, an entity must accept their roles and responsibilities by signing a “OpenPEPPOL Authority Agreement” [PCA] established with the OpenPEPPOL Transport Infrastructure Coordinating Community.

Registration Authorities must abide by all the requirements of the PTN CP and the relevant CPS. RAs may, however implement more restrictive practices based on their internal requirements.

1.5.3 Subscribers

The Subject of a certificate will be the OpenPEPPOL infrastructure service components (Access Point, Service Metadata Publisher or Security Token Service) operated by an OpenPEPPOL Service Provider.

The Subscriber is the Service Provider organization (private company or government institution) who is operating one of the above mentioned OpenPEPPOL infrastructure services. Certificates can only be requested by authorized employees or contractors of these organizations.

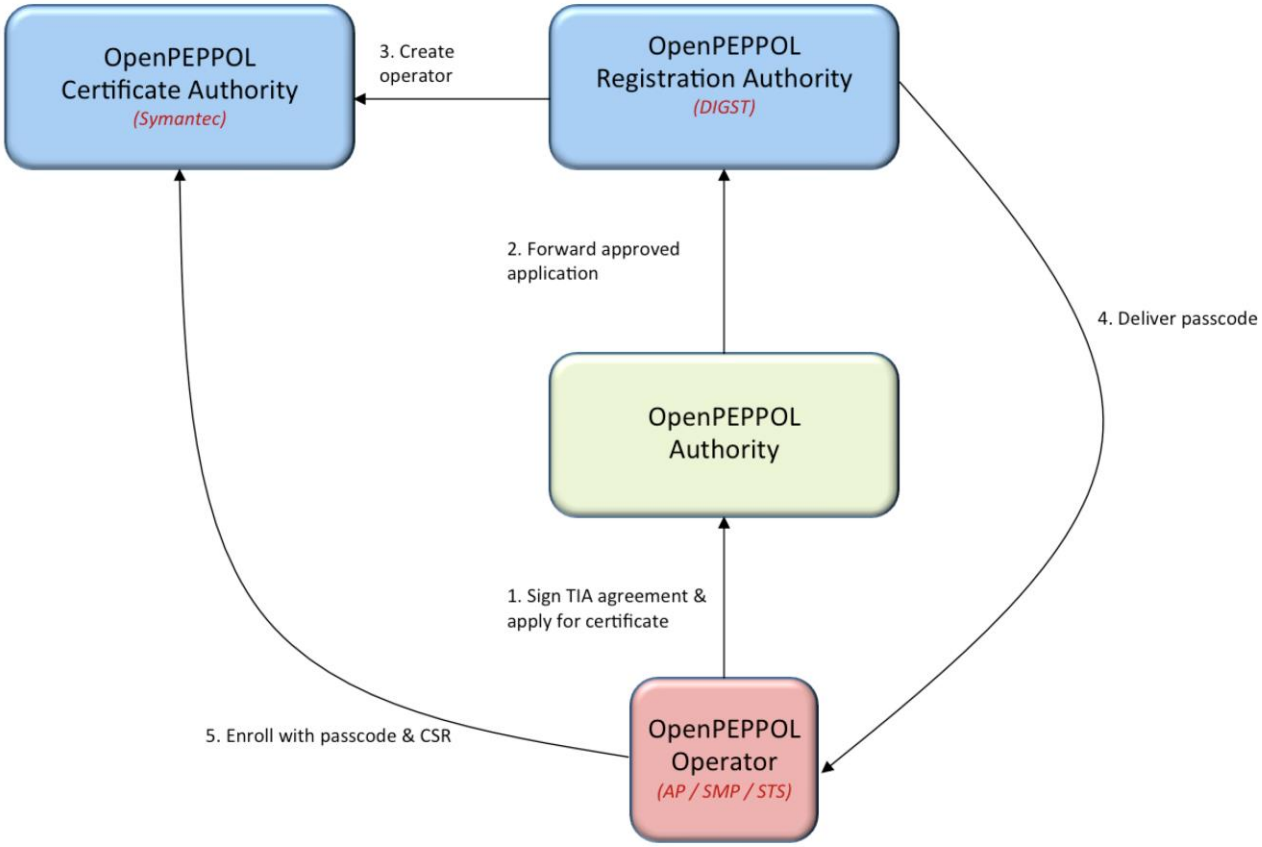
1.5.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under the PTN. A Relying party may, or may not also be a Subscriber within the PTN.

Relying parties of OpenPEPPOL certificates will include both OpenPEPPOL Service Providers as well as government institutions and private companies who use the OpenPEPPOL infrastructure for eProcurement transactions.

1.5.5 Enrollment Process Overview

To show how the different entities work together, the figure below illustrates the enrollment process:



The OpenPEPPOL Authority processes applicant requests within their country or region for OpenPEPPOL operators. The Authority is responsible for

- Validating the applicant as a registered organization
- Validating the applicant's identity and authorization to submit the request
- Confirming acceptance of the Provider Agreement
- Retain records of all applications processed.

The applicant is required to accept the terms of the Provider Agreement.

1.6 Certificate Usage

1.6.1 Appropriate Certificate Uses

OpenPEPPOL certificates may only be used within the OpenPEPPOL infrastructure in accordance with the BUSDOX specifications [BUSDOX]:

- OpenPEPPOL Access Point certificates must only be used for transactions defined for OpenPEPPOL Access Point. This involves digital signing, encryption and client authentication.
- OpenPEPPOL Security Token Service certificates must only be used for transactions defined for a OpenPEPPOL Security Token Service. This involves digital signing only.

- OpenPEPPOL Service Metadata Publisher certificate must only be used for transactions defined for a OpenPEPPOL Service Metadata Publisher. This involves digital signing only.

1.6.2 Prohibited Certificate Uses

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

All end entity certificate usage other than that specified in section 1.4.1 is prohibited.

CA Certificates may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

1.7 Policy Administration

1.7.1 Organization Administering the Document

OpenPEPPOL AISBL

1.7.2 Contact Person

OpenPEPPOL Transport Infrastructure Director:
Sven Rostgaard Rasmussen (svrra@digst.dk)

Danish Digitisation Agency, Ministry of Finance
Landgreven 4
1017 Copenhagen K

1.7.3 Person Determining CPS Suitability for the Policy

The OpenPEPPOL Transport Infrastructure Coordinating Community determines the suitability and applicability of this CP.

1.7.4 CP Approval Procedures

Approval of this CP and subsequent amendments shall be made by the OpenPEPPOL Transport Infrastructure Coordinating Community. Amendments shall either be in the form of a document containing an amended form of the CP or an update notice. Amended versions or updates shall be published in the OpenPEPPOL website at www.peppol.eu

Updates supersede any designated or conflicting provisions of the referenced version of the CP. The OpenPEPPOL Transport Infrastructure Coordinating Community shall determine whether changes to the CP require a change in the Certificate policy object identifiers of the Certificate policies.

1.8 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions.

2 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

OpenPEPPOL is responsible for maintaining a publicly accessible online repository and has entered an agreement with Symantec to operate the repositories on its behalf.

2.2 Publication of Certification Information

Symantec will on OpenPEPPOL's behalf maintain a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information.

OpenPEPPOL CAs publish the Certificates they issue on behalf of their own CAs. Upon revocation of an end-user Subscriber's Certificate, the CA that issued the Certificate shall publish notice of such revocation in the repository. In addition, CA shall issue Certificate Revocation Lists (CRLs) and provide OCSP services (Online Certificate Status Protocol.) for their own CAs.

OpenPEPPOL will at all times publish a current version of:

- This PTN CP

2.3 Time or Frequency of Publication

CA information is published promptly after it is made available to the CA. The PTN offers CRLs showing the revocation of PTN Certificates and offers status checking services through the Symantec Repository. CRLs for end-user Subscriber Certificates shall be issued at least once per day.

CRLs for the PTN Root CA is published quarterly and also whenever a CA Certificate is revoked.
If a Certificate listed in a CRL expires, it may be removed from later issued CRLs after the Certificate's expiration.

2.4 Access Controls on Repositories

OpenPEPPOL shall not intentionally use technical means of limiting access to this CP, their CPS, Certificates, Certificate status information, or CRLs. OpenPEPPOL shall implement controls to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Unless where indicated otherwise in this CP, the relevant CPS or the content of the digital certificate, names appearing in Certificates issued under PTN are authenticated.

3.1.1 Types of Names

OpenPEPPOL Subscriber Certificates contain an X.501 distinguished name (DN) in the Subject name field.

The Subject name field will contain a unique identifier to the service provider when they apply for a OpenPEPPOL certificate as well as information on the organization operating the service. The certificate is thus service specific but not server specific and can be re-used among multiple servers (e.g. in a cluster).

The CN component will contain a 10 digit number assigned by the RA and a prefix stating the type of service provider (Access Point, Service Metadata Publisher or Security Token Service) e.g.:

- CN=APP_1000000015
- CN=SMP_2000000015

- CN=STS_3000000015

The 10-digit number for Access Point certificates will begin with the number 1 as the first digit, SMP certificates will begin with the number 2, and STS certificates will begin with the number 3.

The (O=) component shall be the legal name of the organization running the service (i.e. the service provider organization). The organization name will be authenticated.

The (C=) country component shall be the 2-character ISO country code where the service provider organization is registered.

The DN shall not include the organizational unit (OU=) component.

3.1.2 Need for Names to be Meaningful

OpenPEPPOL Subscriber Certificates shall include meaningful names in the following sense: they shall contain names with commonly understood semantics permitting the determination of the identity of the organization that is listed in the (O=) field in the Certificate. The Subject field will identify a unique service in the OpenPEPPOL infrastructure and the DN can be used to refer to that service.

3.1.3 Anonymity or Pseudonymity of Subscribers

OpenPEPPOL does not allow anonymity or pseudonymity of service providers / services in certificates since the (O=) component contains the legal name of the organization.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation

3.1.5 Uniqueness of Names

The names of Subscribers within the PTN shall be unique. Certificates shall only be issued with a unique DN. It is *not* possible for a Subscriber to be issued two or more certificates with the same Subject Distinguished Name.

3.1.6 Recognition, Authentication, and Role of Trademarks

OpenPEPPOL shall not be required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. OpenPEPPOL shall be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another OpenPEPPOL-approved method.

3.2.2 Authentication of Organization Identity

OpenPEPPOL certificates contain an organization name attribute.The identity of the organization and other enrollment information provided by Certificate Applicants is confirmed in accordance with the procedures set forth in OpenPEPPOL's documented Validation Procedures.

At a minimum, OpenPEPPOL Authorities shall:

- determine that the organization exists by reviewing organizational documentation issued by or filed with the applicable government agency or recognized authority that confirms the existence of the organization,
- confirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so

3.2.3 Authentication of Individual Identity

OpenPEPPOL certificates do not contain individual identity – the service named in the Subject field is assigned a prefix and a unique number by OpenPEPPOL as part of processing the application.

3.2.4 Non-Verified Subscriber Information

No such information is present in OpenPEPPOL Certificates.

3.2.5 Validation of Authority

The OpenPEPPOL Authority must verify that the person submitting an application for a certificate is authorized to do so by the service provider organization. The individual may be an authorized employee in the service provider organization or an authorized contractor.

3.2.6 Criteria for Interoperation

Only CAs approved by the OpenPEPPOL Transport Infrastructure Coordinating Community are authorized for interoperation within the OpenPEPPOL PKI.

The following constraints apply to OpenPEPPOL Certificates:

- Certificates issued by the OpenPEPPOL Access Point Sub CA must only be used for OpenPEPPOL Access Point services for the specific operations describes in [BUSDOX].
- Certificates issued by the OpenPEPPOL Service Metadata Publisher Sub CA must only be used for OpenPEPPOL Service Metadata Publisher services for the specific operations describes in [BUSDOX].
- Certificates issued by the OpenPEPPOL Security Token Service Sub CA must only be used for OpenPEPPOL Security Token Services for signing SAML Assertions as described in [BUSDOX].

OpenPEPPOL Service Providers must use software that correctly implements the BUSDOX standards and OpenPEPPOL Service Standard mentioned above.

3.3 Identification and Authentication for Re-Key Requests

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. CAs and RAs require that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey").

Renewal of certificates without generation of new keys is not allowed.

3.3.1 Identification and Authentication for Routine Re-Key

The OpenPEPPOL Authority approving a Certificate Application for the Subscriber of an end-user Subscriber Certificate shall be responsible for authenticating a request for re-key. Re-key procedures ensure that the person or organization seeking to rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit a Challenge Phrase with their enrollment information. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including contact information) has not changed, a renewal Certificate is automatically issued.

After rekeying in this fashion, every second instance of subsequent rekeying thereafter, the CA or RA reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements of an original Certificate Application.

3.3.2 Identification and Authentication for Re-Key After Revocation

Re-key/renewal after revocation is not permitted if the revocation occurred because:

- the Certificate was issued to an organization other than the one named as the Subject of the Certificate, or
- the Certificate was issued without the authorization of the organization or entity named as the Subject of such Certificate, or
- the entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false
- the certificate was deemed harmful to the PTN.

Subject to the foregoing paragraph, renewal of an organizational or CA Certificate following revocation of the Certificate is permissible as long as renewal procedures ensure that the organization or CA seeking renewal is in fact the Subscriber of the Certificate.

Renewed organizational Certificates shall contain the same Subject distinguished name as the Subject distinguished name of the organizational Certificate being renewed. Other than this procedure the requirements for the identification and authentication of an original Certificate Application shall be used for renewing a Certificate following revocation.

3.4 Identification and Authentication for Revocation Request

Prior to revocation of any Certificate, revocation procedures ensure that the revocation has in fact been requested by the Certificate's Subscriber, the entity that approved the Certificate Application or the OpenPEPPOL Transport Infrastructure Coordinating Community. The OpenPEPPOL Transport Infrastructure Coordinating Community can choose to revoke as OpenPEPPOL Service Provider Certificate in the event that the service provider fails to comply with the OpenPEPPOL AP or SMP Provider Agreements ([APA] or [SMPA]).

Acceptable procedures for authenticating the revocation requests of a Subscriber include:

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record
- Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,
- Communication with the Subscriber providing reasonable assurances that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

OpenPEPPOL Authorities are entitled to request the revocation of end-user Subscriber Certificates within their country / region.

CA certificates can only be revoked by OpenPEPPOL Transport Infrastructure Coordinating Community.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

People who may submit certificate applications include:

- Any authorized representative of an Organization that has signed the OpenPEPPOL AP Provider Agreement [APA] or OpenPEPPOL SMP Provider Agreement [SMPA].

4.1.2 Enrolment Process and Responsibilities

Certificate Subscribers
All Certificate Subscribers shall undergo an enrollment process consisting of:

- completing a Certificate Application and providing true and correct information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key
- demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to the CA

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

An RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2

4.2.2 Approval or Rejection of Certificate Applications

An RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2
- The Subscriber has entered a valid provider agreement with the OpenPEPPOL Authority regarding the operating of a OpenPEPPOL infrastructure service.
- The Subscriber satisfies other criteria defined by the OpenPEPPOL Transport Infrastructure Coordinating Community required for operating OpenPEPPOL infrastructure services.

An RA will reject a certificate application if:

- identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time

4.2.3 Time to Process Certificate Applications

CAs and RAs begin processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless. A certificate application remains active until rejected.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

A Certificate is created and issued following approval of a Certificate Application received in a request from a OpenPEPPOL Authority. The CA creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs issuing Certificates to end-user Subscribers shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available and the means for obtaining them. Certificates shall be made available to end-user Subscribers, by allowing them to download them from a web site.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Downloading a Certificate or installing a Certificate from a message attachment constitutes the Subscriber's acceptance of the Certificate.
- Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

The PTN publishes the Certificates they issue in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the Private key corresponding to the public key in the certificate shall only be permitted once the Subscriber has accepted the certificate. The certificate shall be used lawfully in accordance with OpenPEPPOL's AP/SMP Provider Agreements, the terms of this CP and the relevant CPS.

Certificate use must be consistent with the KeyUsage field extensions included in the certificate (e.g., if digital signature is not enabled then the certificate must not be used for signing). Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

Certificates must only be used for the purposes listed in sections 1.4.1 and 3.2.6.

4.5.2 Relying Party Public Key and Certificate Usage

Reliance on a certificate must be reasonable under the circumstances.

Certificates must only be relied upon for transactions defined in the [BUSDOX] specifications and only after all validation steps described herein are performed.

Before any act of reliance, Relying Parties shall independently assess:

- The appropriateness of the use of a Certificate as specified by the above standards.
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate (e.g., if digital signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether it is reasonable to rely on a digital signature performed prior to revocation of a Certificate in the Certificate chain. Any such reliance is made solely at the risk of the Relying Party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate to the Subscriber without changing the public key or any other information in the certificate. Certificate renewal is not supported for OpenPEPPOL certificates as new keys must always be generated through Certificate Re-Key.

4.6.1 Circumstances for Certificate Renewal

No stipulation.

4.6.2 Who May Request Renewal

No stipulation.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-Key

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key. Certificate rekey is supported for all types of OpenPEPPOL certificates.

4.7.1 Circumstances for Certificate Re-Key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. A certificate may also be rekeyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

Only an authorized representative for an organization may request certificate renewal.

4.7.3 Processing Certificate Re-Keying Requests

Re-key procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

Refer to section 3.3.1 for authentication of re-keying requests.
A Certificate cannot be re-keyed if the Subscribers enrollment information has changed.

Re-keying will only be permitted once.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting acceptance of a re-keyed certificate is in accordance with Section 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

The re-keyed certificate is published in the issuing CAs publicly accessible repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs will receive notification of the issuance of certificates they approve.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the Subscriber's public key). Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1

4.8.3 Processing Certificate Modification Requests

An RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Only in the circumstances listed below, will an end-user Subscriber certificate be revoked and published on a CRL. Upon request from a Subscriber who can no longer use (or no longer wishes to use) a certificate for a reason other than one mentioned below, OpenPEPPOL will flag the certificate as inactive in its database but will not publish the certificate on a CRL.

An end-user Subscriber Certificate is revoked if:
• A Subscriber, a OpenPEPPOL Authority or the OpenPEPPOL Transport Infrastructure Coordinating Community has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,
• A OpenPEPPOL Authority or Transport Infrastructure Coordinating Community has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable OpenPEPPOL AP/SMP provider agreement,
• The OpenPEPPOL AP/SMP Provider Agreement with the Subscriber has been terminated,
• An OpenPEPPOL Authority, Customer or OpenPEPPOL Transport Infrastructure Coordinating Community has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate was issued to a person other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person named as the Subject of such Certificate,
• A OpenPEPPOL Authority or OpenPEPPOL Transport Infrastructure Coordinating Community has reason to believe that a material fact in the Certificate Application is false,
• An OpenPEPPOL Authority or OpenPEPPOL Transport Infrastructure Coordinating Community determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
• The Subscriber's organization name changes,
• The information within the Certificate, other than Nonverified Subscriber Information, is incorrect or has changed, or
• The continued use of that certificate is harmful to the PTN.

When considering whether certificate usage is harmful to the PTN, a CA and/or RA considers, among other things, the following:
• The nature and number of complaints received
• The identity of the complainant(s)
• Relevant legislation in force
• Responses to the alleged harmful use from the Subscriber

OpenPEPPOL AP/SMP Provider Agreements require end-user Subscribers to immediately notify the OpenPEPPOL Authority of a known or suspected compromise of its private key.

4.9.2 Who Can Request Revocation

A duly authorized representative of the organization shall be entitled to request the revocation of Certificates issued to the organization. A duly authorized representative of OpenPEPPOL Transport Infrastructure

Coordinating Community or OpenPEPPOL Authority shall be entitled to request the revocation of a Certificate.

Only the OpenPEPPOL Transport Infrastructure Coordinating Community is entitled to request or initiate the revocation of the Certificates issued to its own CAs.

4.9.3 Procedure for Revocation Request

Prior to the revocation of a Certificate, the CA verifies that the revocation has been requested by the Certificate's Subscriber, or the entity that approved the Certificate Application. Refer to section 3.4 for information on how to authenticate revocation requests.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

4.9.5 Time within Which CA Must Process the Revocation Request

Commercially reasonable steps are taken to process revocation requests without delay.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties must perform revocation checks when specified in [BUSDOX].

One method by which the Relying Party may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, the Relying Party may meet this requirement by using OCSP.

PTN will support both CRL and OCSP as mechanisms for revocation checks.

CAs shall publish information on how to find the appropriate CRL or OCSP responder to check for revocation status.

4.9.7 CRL Issuance Frequency (If Applicable)

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates shall be issued at least quarterly but also whenever a CA Certificate is revoked. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation. This is generally done automatically within minutes of generation.

4.9.9 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via OCSP.

4.9.10 On-line Revocation Checking Requirements

A Relying Party may check the status of a Certificate online either by consulting the most recent relevant CRL or by requesting Certificate status using the applicable OCSP responder.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable

4.9.12 Special Requirements Regarding Key Compromise

The PTN will publish information on OpenPEPPOL web sites to notify potential Relying Parties if they discover, or have reason to believe, that there has been a compromise of the private key of one of their components.

OpenPEPPOL will notify Relying Parties via its web site if a PTN CA is compromised and the PTN Root CA shall immediately publish the CA certificate revocation via the Authority Revocation List.

4.9.13 Circumstances for Suspension

The PTN shall not support Certificate Suspension.

4.9.14 Who Can Request Suspension

No stipulation. .

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Certificate Revocation Status of public certificates is available via an LDAP directory (CRL), HTTP download of CRL and via an OCSP Responder.

4.10.2 Service Availability

Certificate Status Services shall be available 24x7 without scheduled interruption.

4.10.3 Optional Features

4.11 End of Subscription

A Subscriber may end a subscription for a PTN certificate by:
• Allowing his/her/its certificate to expire without re-keying that certificate
• Revoking of his/her/its certificate before certificate expiration without replacing the certificates.

4.12 Key Escrow and Recovery

Key escrow will not be used in the PTN.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

All PTN CA and RA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

OpenPEPPOL requirements are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door or gate that provides mandatory access control for individuals and requires a positive response (e.g., door or gate unlocks or opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access. Moreover, each physical security tier encapsulates the next inner tier, such that an inner tier must be fully contained in an outside tier and cannot have a common outside wall with the outside tier, the outermost tier being the outside wall of the building.

The PTN CA shall describe its Site Location and Construction in more detail in their CPS.

5.1.2 Physical Access

Access to each tier of physical security shall be auditable and controlled so that each tier can be accessed only by authorized personnel.

5.1.3 Power and Air Conditioning

The secure facilities of the PTN CA shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities shall be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

The secure facilities of CAs shall be constructed and equipped, and procedures shall be implemented, to prevent floods or other damaging exposure to water.

5.1.5 Fire Prevention and Protection

The secure facilities of CAs shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations.

5.1.6 Media Storage

CAs and RAs shall protect the magnetic media holding backups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

5.1.7 Waste Disposal

CAs shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

5.1.8 Off-Site Backup

CAs shall maintain backups of critical system data or any other sensitive information, including audit data, in a secure off-site facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Employees, contractors, and consultants that are designated to manage infrastructural trustworthiness shall be considered to be “Trusted Persons” serving in a “Trusted Position.” Persons seeking to become Trusted Persons by obtaining a Trusted Position shall meet the screening requirements of this CP.

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including (in the case of CAs) personnel having access to restricted portions of its repository or the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

5.2.2 Number of Persons Required Per Task

CAs shall establish, maintain, and enforce rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold “Secret Shares” and vice versa.

Other manual operations require the participation of at least two Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process.

5.2.3 Identification and Authentication for Each Role

The CA and RAs shall confirm the identity and authorization of all personnel seeking to become Trusted before such personnel are:

- issued with their access devices and granted access to the required facilities;
- given electronic credentials to access and perform specific functions on Information Systems and CA or RA systems.

The PTN shall authenticate the identity of persons assigned to Trusted Roles.
Identity authentication shall include a check of well-recognized forms of identification, such as passports and driver's licenses. Identity shall be further confirmed through background the checking procedures specified in this CP.

The organization that operates an RA shall sign the OpenPEPPOL Authority Agreement [PCA] with the OpenPEPPOL Transport Infrastructure Coordinating Community as described in section 1.3.2 and shall perform identification and authentication of personnel prior to being assigned to the RA Trusted Role.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to)

- the generation, issuing or destruction of a CA certificate
- the loading of a CA on production

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Personnel seeking to become Trusted Persons shall present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

5.3.2 Background Check Procedures

Persons seeking to become Trusted Persons shall undergo successful background checks. Background checks shall be repeated for personnel holding Trusted Positions at least every five (5) years. These procedures shall be subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law, the investigating entity shall utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable professional references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information shall be evaluated by human resources and security personnel, and such personnel shall take actions that are reasonable in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons. The use of information revealed in a background check to take such actions shall be subject to applicable law.

Background investigation of persons seeking to become a Trusted Person includes:

- a confirmation of previous employment,
- a check of professional references,
- a confirmation of the highest or most relevant educational degree obtained,
- a search of criminal records (local, state or provincial, and national), and
- a check of credit/financial records.

The following additional investigations shall also be performed:

- a search of driver's license records, and
- a search of government social insurance records (analogous to Social Security Administration records in the United States or comparable system outside the United States).

5.3.3 Training Requirements

Personnel shall be provided with the requisite training needed to perform their job responsibilities relating to CA or RA operations competently and satisfactorily. Training shall be periodically reviewed to remain current and adequate.

5.3.4 Retraining Frequency and Requirements

The CA shall provide refresher training and updates to their personnel to the extent and frequency required to ensure that personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The CA and RAs shall establish, maintain, and enforce employment policies for the discipline of personnel following unauthorized actions. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

The CA and RAs may permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly-defined outsourcing relationships and only under the following conditions:

- the entity using the independent contractors or consultants as Trusted Persons does not have suitable employees available to fill the roles of Trusted Persons, and
- the contractors or consultants are trusted by the entity to the same extent as if they were employees.

5.3.8 Documentation Supplied to Personnel

The CA and RAs shall provide their personnel (including Trusted Persons) with the requisite training and access to other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The types of auditable events that must be recorded by the CA and RAs are set forth below. All logs, whether electronic or manual, shall contain the date and time of the event, and the identity of the entity that caused the event. The CPS shall state the logs and types of events recorded.

Types of auditable events include:

- Operational events (including but not limited to (1) the generation of a CA's own keys and the keys of subordinate CAs, (2) start-up and shutdown of systems and applications, (3) changes to CA details or keys, (4) cryptographic module lifecycle management-related events (*e.g.*, receipt, use, deinstallation, and retirement), (5) possession of activation data for CA private key operations, physical access logs, (6) system configuration changes and maintenance, (7) Records of the destruction of media containing key material, activation data, or personal Subscriber information)
- Certificate lifecycle events (including but not limited to initial issuance, re-key, renew, revocation, suspension)
- Trusted employee events (including but not limited to (1) logon and logoff attempts, (2) attempts to create, remove, set passwords or change the system privileges of the privileged users, (3) personnel changes)
- Discrepancy and compromise reports (including but not limited to unauthorized system and network logon attempts)
- Failed read and write operations on the Certificate and repository
- Changes to Certificate creation policies e.g., validity period

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed in response to alerts based on irregularities and incidents within the CA/RA systems. The CA shall compare the audit logs with the supporting manual and electronic logs from the RA when any action is deemed suspicious.

Audit log processing shall consist of a review of the audit logs and documenting the reason for all significant events in an audit log summary. Audit log reviews shall include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews shall be documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

5.4.6 Audit Collection System (Internal vs. External)

No stipulation

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the entity that caused the event.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments ("LSVAs") are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. An annual LSVA will be an input into the PTN's annual Compliance Audit.

5.5 Records Archival

5.5.1 Types of Records Archived

The CA and RAs archive:

- All audit data collected in terms of Section 5.4
- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

5.5.2 Retention Period for Archive

Records shall be retained for at least two years.

5.5.3 Protection of Archive

The CA and RAs shall protect the archive so that only their authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CP.

5.5.4 Archive Backup Procedures

Entities compiling electronic information shall incrementally backup system archives of such information on a daily basis and perform full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive Collection System (Internal vs. External)

Archive collection systems for entities within the PTN shall be internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

The PTN Root CA shall conduct a Key Generation Ceremony in order to generate a new key pair for the PTN subordinate CA. During such Key Generation Ceremony, the Root CA shall sign and issue the CA a new Certificate. Such Key Generation Ceremony shall meet the Key Ceremony requirements documented in the PTN's confidential security policies. New CA Certificates containing the new CA public keys generated during such Key Generation Ceremony shall be made available to Relying Parties.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with CP § 6.2.4.

5.7.2 Computing Resources, Software and/or Data are Corrupted

Following corruption of computing resources, software, and/or data, a report of the incident and a response to the event, shall be promptly made by the affected CA or RA. The CPS shall describe the reporting and handling procedures to be performed.

5.7.3 Entity Private Key Compromise Procedures

In the event of a CA private key compromise that CA will be revoked. The PTN uses commercially reasonable efforts to notify potential Relying Parties if they discover, or have reason to believe, that there has been a Compromise of the private key of a CA.

5.7.4 Business Continuity Capabilities after a Disaster

PTN entities operating secure facilities for CA and RA operations develop, test, maintain and, if necessary, implement a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster. Disaster recovery plans address the restoration of information systems services and key business functions. Disaster recovery sites have the equivalent physical security protections specified by the PTN.

The CA has the capability of restoring or recovering essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions: Certificate issuance, Certificate revocation, publication of revocation information. The CA's disaster recovery database shall be synchronized with the production database within the time limits set forth in the Security and Audit Requirements Guide. The CA's disaster recovery equipment shall have the physical security protections documented in the PTN's confidential security policies, which includes the enforcement of physical security tiers.

5.8 CA or RA Termination

OpenPEPPOL CAs are terminated when the agreement between the OpenPEPPOL Transport Infrastructure Coordinating Community and the CA operator is terminated or expires.

The termination plan may cover issues such as:

- Providing notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers,
- Handling of the cost of such notice,
- If the successor CA is within the jurisdiction of the OpenPEPPOL Transport Infrastructure Coordinating Community, assistance with a user migration plan,
- The revocation of the Certificate issued to the CA by the Superior Entity,
- The preservation of the CA's archives and records for the time periods required in this CP
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- The refund (if necessary) to Subscribers whose unexpired, unrevoked Certificates are revoked under the termination plan or provision, for the issuance of substitute Certificates by a successor CA,
- Disposition of the CA's private key and the hardware token containing such private key,
- Provisions needed for the transition of the CA's services to a successor CA.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pair generation shall be performed using Trustworthy Systems and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys. This requirement applies to end-user Subscribers.

CA keys are generated in a Key Generation Ceremony. All Key Generation Ceremonies conform to the requirements documented in the PTN's confidential security policies.

6.1.2 Private Key Delivery to Subscriber

End-user Subscribers' private keys are generated by the end-user Subscribers themselves, and therefore private key delivery to a Subscriber is not necessary.

6.1.3 Public Key Delivery to Certificate Issuer

When a public key is transferred to the issuing CA to be certified, it shall be delivered through a mechanism ensuring that the public key has not been altered during transit and that the Certificate Applicant possesses the private key corresponding to the transferred public key. The acceptable mechanism within the PTN for public key delivery is a PKCS#10 Certificate signing request package or an equivalent method ensuring that:

- The public key has not been altered during transit; and
- The Certificate Applicant possesses the private key corresponding to the transferred public key.

6.1.4 CA Public Key Delivery to Relying Parties

The OpenPEPPOL CA certificates (Root and three subordinate CA certificates) will be published on OpenPEPPOL web sites.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The current PTN Standard for minimum key sizes is the use of key pairs equivalent in strength to 2048 bit RSA for CAs.

6.1.6 Public Key Parameters Generation and Quality Checking

PTN Participants using the Digital Signature Standard shall generate the required Key Parameters in accordance with FIPS 186-2 or a OpenPEPPOL approved equivalent standard.

When PTN Participants use the Digital Signature Standard, the quality of the generated Key Parameters shall be verified in accordance with FIPS 186-2 or a OpenPEPPOL-approved equivalent standard.

6.1.7 Key Usage Purposes (as per x509v3 field)

Refer to Section 7.1.2.1.

6.2 Private Key Protection & Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Private keys within the PTN shall be protected using a Trustworthy System and private key holders shall take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such private keys in accordance with this CP, contractual obligations and requirements documented in the PTN's confidential security policies. End-user Subscribers have the option of protecting their private keys in a smart card or other hardware token.

CAs shall perform all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-1 level 3. All RA cryptographic operations shall be performed on a cryptographic module rated at FIPS 140-1 level 2.

6.2.2 Private Key (n out of m) Multi-Person Control

Multi-person control are enforced to protect the activation data needed to activate CA private keys held by CAs in accordance with the standards documented in the PTN's confidential security policies. CAs use "Secret Sharing" to split the private key or activation data needed to operate the private key into separate parts called "Secret Shares" held by individuals called "Shareholders." Some threshold number of Secret Shares (m) out of the total number of Secret Shares (n) shall be required to operate the private key.

The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same.

6.2.3 Private Key Escrow

Neither CA private keys nor subscriber private keys are escrowed in OpenPEPPOL.

6.2.4 Private Key Backup

CAs shall back up their own private keys so as to be able to recover from disasters and equipment malfunction in accordance with the standards documented in the PTN's confidential security policies. Backups shall be made in accordance with these documented policies. Back-ups shall be made by copying

such private keys and entering them onto back-up cryptographic modules in accordance with Section 6.2.6 and 6.2.7.

Private keys that are backed up are to be protected from unauthorized modification or disclosure through physical or cryptographic means. Backups are protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within the CA site, such as at a disaster recovery site or at another secure off-site facility, such as a bank safe.

6.2.5 Private Key Archival

Upon expiration of a OpenPEPPOL CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 2 years using hardware cryptographic modules that meet the requirements of this CPS. These CA key pairs shall not be used for any signing events after their expiration date, unless the CA Certificate has been renewed in terms of this CPS.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Entry of a private key into a cryptographic module shall use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

CAs generating CA or RA private keys on one hardware cryptographic module and transferring them into another shall securely transfer such private keys into the second cryptographic module to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. Such transfers shall be limited to making backup copies of the private keys on tokens in accordance with the standards documented in the PTN's confidential security policies. Private keys shall be encrypted during such transfer.

6.2.7 Private Key Storage on Cryptographic Module

CA private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8 Method of Activating Private Key

All PTN Participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

The PTN Standard for private key protection (other than RAs) is for Subscribers to:

• Use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, a network logon password
• Take commercially reasonable measures for the physical protection of the Subscriber's workstation or server to prevent use of the workstation / server and its associated private key without the Subscriber's authorization.
When deactivated, private keys shall be kept in encrypted form only.

An online CA's private key shall be activated by a threshold number of Shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline. Similarly, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA's private key. Once the private key is activated, it shall be active only for one time.

6.2.9 Method of Deactivating Private Key

Subscribers have an obligation to protect their private keys. Such obligations extend to protection of the private key after a private key operation has taken place. The private key may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user.

When deactivated, private keys shall be kept in encrypted form only.

When an online CA is taken offline by a CA, the CA personnel shall remove the token containing such CA's private key from the reader in order to deactivate it. With respect to the private keys of offline CAs, after the completion of a Key Generation Ceremony, in which such private keys are used for private key operations, the CA's personnel shall remove the token containing such CAs' private keys from the reader in order to deactivate them. Once removed from the reader, tokens shall be protected.

6.2.10 Method of Destroying Private Key

Where required, CA private keys are destroyed in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of the key. CA personnel decommission the CA's private key by deleting it using functionality of the token containing such CA's private key so as to prevent its recovery following deletion, while not adversely affecting the private keys of other CAs contained on the token. This process shall be witnessed in accordance with the standards documented in the PTN's confidential security policies.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The PTN shall archive their public keys.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period for Certificates shall be set according to the time limits set forth in Table 4 below.

The usage period for end-user Subscriber key pairs is the same as the Operational Period for their Certificates, except that private keys may continue to be used after the Operational Period for decryption. The Operational Period of a Certificate ends upon its expiration or revocation. A CA shall not issue Certificates if their Operational Periods would extend beyond the usage period of the key pair of the CA. Therefore, the CA key pair usage period is necessarily shorter than the operational period of the CA Certificate.

Specifically, the usage period is the Operational Period of the CA Certificate minus the Operational Period of the Certificates that the CA issues. Upon the end of the usage period for a Subscriber or CA key pair, the Subscriber or CA shall thereafter cease all use of the key pair, except to the extent a CA needs to sign revocation information until the end of the Operational Period of the last Certificate it has issued.

Certificate	Validity Period
OpenPEPPOL self-signed Root CA	Ten years
Root CA issued OpenPEPPOL Access Point CA	Five years
Root CA issued OpenPEPPOL Service Metadata Publisher CA	Five years
Root CA issued OpenPEPPOL Security Token Service CA	Five years
Online CA issued End-user individual Subscriber	Two years.
Online CA issued OCSP Responder certificates	Two years

Table 4 – Certificate Operational Periods

Except as noted in this section, PTN participants shall cease all use of their key pairs after their usage periods have expired.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

To the extent passwords are used as activation data, Subscribers shall generate passwords that cannot easily be guessed or cracked by dictionary attacks. Subscribers may not need to generate activation data, for example if they use biometric access devices.

CAs generate activation data for their own CAs' private keys, in accordance with the Secret Sharing requirements of this CP and the standards documented in the PTN's confidential security policies.

6.4.2 Activation Data Protection

End-user Subscribers shall protect the activation data for their private keys, if any, to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

The CAs utilize Secret Sharing in accordance with this CP and the standards documented in the PTN's confidential security policies. CAs provide the procedures and means to enable Shareholders to take the precautions necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of the Secret Shares that they possess. Shareholders shall not:

- Copy, disclose, or make the Secret Share available to a third party, or make any unauthorized use of it whatsoever; or
- disclose his, her, or any other person's status as a Shareholder to any third party.

The Secret Shares and any information disclosed to the Shareholder in connection with his or her duties as a Shareholder constitute Confidential/Private Information.

The CA includes in their disaster recovery plans provisions for Shareholders making their Secret Shares available at a disaster recovery site after a disaster.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

No stipulation.

6.4.3.2 Activation Data Destruction

Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapses, CAs shall decommission activation data by overwriting and/or physical destruction. See also section 6.2.10.

6.5 Computer Security Controls

CA and RA functions take place on Trustworthy Systems in accordance with the standards documented in the PTN's confidential security policies.

6.5.1 Specific Computer Security Technical Requirements

CAs shall ensure that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 5.4.1. In addition, CAs limit access to production servers to those individuals with a valid business reason for access. General application users shall not have accounts on the Production servers.

CAs shall have production networks logically separated from other components. This separation prevents network access except through defined application processes. CAs shall use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems. CAs shall require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and shall require that passwords be changed on a periodic basis and whenever necessary. Direct access to a CA's database maintaining the CA's repository shall be limited to Trusted Persons in the CA operations group having a valid business reason for such access.

RAs shall ensure that the systems maintaining RA software and data files are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 5.4.1.

RAs shall logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. RAs shall use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information. RAs shall require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and shall require that passwords be changed on a periodic basis and as necessary. Direct access to the RA's database maintaining Subscriber information shall be limited to Trusted Persons in the RA's operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

Specific security sensitive areas of the CA and RA functionality of software supplied by the PKI Provider shall meet the assurance requirements of EAL 3 (Common Criteria for Information Technology Security Evaluation, v 2.1, Aug. 1999).

6.6 Life cycle Technical Controls

6.6.1 System Development Controls

CA and RA software shall be developed within a systems development environments that meet Symantec's development assurance requirements. The software provider shall use a design and development process that enforces quality assurance and process correctness.

The software, when first loaded, shall provide a method for the entity to verify that the software on the system:

- originated from the software provider,
- has not been modified prior to installation, and
- is the version intended for use

6.6.2 Security Management Controls

Software for CA and RA functions used to manage OpenPEPPOL Certificates shall be subject to checks to verify its integrity. The software provider shall provide a hash of all software packages or software updates it provides. This hash can be used to verify the integrity of such software manually. CAs shall also have mechanisms and/or policies in place to control and monitor the configuration of their CA systems. Upon installation, and at least once a day, CAs shall validate the integrity of the CA system.

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

CA and RA functions are performed using networks secured in accordance with the standards documented in the PTN's confidential security policies to prevent unauthorized access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

PTN Certificates generally conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280").

At a minimum, X.509 PTN Certificates shall contain the basic fields and indicated prescribed values or value constraints in Table 5 below:

Field	Value or Value constraint
Serial Number	Unique positive integer
Signature Algorithm	Object identifier of the algorithm used to sign the certificate (See CP § 7.1.3)
Issuer DN	See Section 7.1.4
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.
Subject DN	See CP § 7.1.4
Subject Public Key	Encoded in accordance with RFC 5280
Signature	Generated and encoded in accordance with RFC 5280

Table 5 – Certificate Profile Basic Fields

7.1.1 Version Number(s)

All PTN Certificates shall be X.509 Version 3 Certificates.

7.1.2 Certificate Extensions

The CAs shall populate X.509 Version 3 PTN Certificates with the extensions required by Section 7.1.2.1-7.1.2.8. Private extensions are not permissible.

7.1.2.1 Key Usage

X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002. The KeyUsage extension in X.509 Version 3 PTN Certificates are configured so as to set and clear bits and the criticality field in accordance with Table 6 below. The criticality field of the KeyUsage extension is set to FALSE for end entity Subscriber certificates, but TRUE for CA certificates.

		OpenPEPPOL CAs	OpenPEPPOL End Entity Service Provider Certificates
Criticality		**TRUE**	**FALSE**
0	digitalSignature	–	Set
1	nonRepudiation	–	–
2	keyEncipherment	–	Set
3	dataEncipherment	–	Set
4	keyAgreement	–	Set
5	keyCertSign	Set	–
6	CRLSign	Set	–
7	encipherOnly	–	–
8	decipherOnly	–	–

Table 6 – Settings for KeyUsage Extension

The nonRepudiation bit is not set in PTN certificates.

7.1.2.2 Certificate Policies Extension

CertificatePolicies extension of X.509 Version 3 Certificates are populated with the object identifier of this CP in accordance with Section 7.1.6 and with policy qualifiers set forth in Section 7.1.8. The criticality field of this extension shall be set to FALSE.

7.1.2.3 Subject Alternative Names

The subjectAltName extension of X.509 Version 3 Certificates is not used in OpenPEPPOL certificates.

7.1.2.4 Basic Constraints

X.509 Version 3 CA Certificates BasicConstraints extension shall have the CA field set to TRUE and criticality set to TRUE. End-user Subscriber Certificates BasicConstraints extension, shall be populated with a value of an empty sequence and criticality set to FALSE.

X.509 Version 3 CA Certificates shall have a “pathLenConstraint” field of the BasicConstraints extension set to the maximum number of CA certificates that may follow this Certificate in a certification path. The three OpenPEPPOL Subordinate CA Certificates defined in this document shall have a “pathLenConstraint” field set to a value of “0” indicating that only an end-user Subscriber Certificate may follow in the certification path.

7.1.2.5 Extended Key Usage

X.509 Version 3 PTN End-Entity Certificates are populated with an ExtendedKeyUsage extension configured to include the key purpose object identifiers (OID) By default, ExtendedKeyUsage is set as a non-critical extension. PTN CA Certificates do not include the ExtendedKeyUsage extension.

The only extension used for OpenPEPPOL Service Provider Certificates is ClientAuth (1.3.6.1.5.5.7.3.2).

7.1.2.6 CRL Distribution Points

X.509 Version 3 PTN Certificates are populated with a cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the Certificate's status. The criticality field of this extension shall be set to FALSE.

7.1.2.7 OCSP responder extension

The OCSP responder URL is included in the certificate AIA field.

7.1.2.8 Authority Key Identifier

X.509 Version 3 PTN Certificates are populated with an authorityKeyIdentifier extension. The method for generating the keyIdentifier based on the public key of the CA issuing the Certificate shall be derived from the SHA-1 hash of the public key of the Issuer. The criticality field of this extension shall be set to FALSE. Also – the PTN Root CA is a self-signed CA & shall not have an Authority Key Identifier.

7.1.2.9 Subject Key Identifier

The criticality field of this extension in PTN Certificates shall be set to FALSE and the method for generating the keyIdentifier based on the public key of the Subject of the Certificate shall be derived from the SHA-1 hash of the public key.

7.1.3 Algorithm Object Identifiers

PTN Certificates are signed using one of following algorithms.

sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

ecdsa-with-Sha384 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}

Certificate signatures produced using these algorithms shall comply with RFC 3279

7.1.4 Name Forms

PTN Certificates are populated with the name required under Section 3.1.1.

7.1.5 Name Constraints

No stipulation

7.1.6 Certificate Policy Object Identifier

The object identifier for the Certificate policy is set forth in Section 1.2. The CertificatePolicies extension in each X.509 Version 3 PTN Certificate is populated in accordance with Section 1.2.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

X.509 Version 3 PTN Certificates contain a policy qualifier within the Certificate Policies extension. Such Certificates contain a CPS pointer qualifier that points to the applicable CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

CRLs conform to RFC 5280 and contain the basic fields and contents specified in Table 8 below:

Field	Value or Value constraint
Version	See Section 7.2.1.
Signature Algorithm	Algorithm used to sign the CRL. PTN CRLs are signed using sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) in accordance with RFC 3279.
Issuer	Entity who has signed and issued the CRL.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of Section 4.9.7.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 8 – CRL Profile Basic Fields

7.2.1 Version Number(s)

The PTN supports both X.509 Version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

No stipulation

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate. OCSP may be used to validate OpenPEPPOL certificates.

OCSP responders conform to RFC2560.

7.3.1 Version Number(s)

Version 1 of the OCSP specification as defined by RFC2560 is supported.

7.3.2 OCSP Extensions

The OCSP service shall use secure timestamp and validity period to establish the current freshness of each OCSP response. OCSP shall not use a nonce to establish the current freshness of each OCSP response and clients should not expect a nonce in the response to a request that contains a nonce. Instead, clients should use the local clock to check for response freshness.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

OpenPEPPOL (including all service providers and participants) shall undergo a periodic compliance audit ("Compliance Audit") to ensure compliance with PTN Standards after they begin operations.

In addition to these compliance audits, the OpenPEPPOL Transport Infrastructure Coordinating Community shall be entitled to perform other reviews and investigations to ensure the trustworthiness of the PTN, which include, but are not limited to:

- The OpenPEPPOL Transport Infrastructure Coordinating Community shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on itself in the event it has reason to believe that the audited entity has failed to meet PTN Standards, has experienced an incident or compromise, or has acted or failed to act, such that the audited entity's failure, the incident or compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the PTN.

- The OpenPEPPOL Transport Infrastructure Coordinating Community shall be entitled to perform "Supplemental Risk Management Reviews" on itself, following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

- The OpenPEPPOL Transport Infrastructure Coordinating Community shall be entitled to delegate the performance of these audits, reviews, and investigations reviewed, or investigated or to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with OpenPEPPOL and the personnel performing the audit, review, or investigation.

8.1 Frequency or Circumstances of Assessment

Compliance Audits are conducted at least annually at the sole expense of the audited entity.

8.2 Identity/Qualifications of Assessor

A third party auditing firm shall perform the Compliance Audits of OpenPEPPOL service providers including all participating and RA organizations.

Reviews and audits performed by a third party audit firm shall be performed by a certified public accounting firm with demonstrated expertise in computer security or by accredited computer security professionals employed by a competent security consultancy. Such firm shall also have demonstrated expertise in the performance of IT security and PKI compliance audits.

8.3 Assessor's Relationship to Assessed Entity

Compliance Audits performed by third-party audit firms shall be conducted by firms independent of the audited entity. Such firms shall not have a conflict of interest that hinders their ability to perform auditing services.

8.4 Topics Covered by Assessment

Audit topics for each category of entity are set forth below. The audited entity may make a Compliance Audit a module that is part of an overall annual audit of the entity's information systems.

8.4.1 Audit of the PKI Service Provider

The OpenPEPPOL PKI service provider shall be audited pursuant to the guidelines provided in the American Institute of Certificate Public Accounts' Statement on Auditing Standards (SAS) Number 70, *Reports on* the Processing of Transactions by Service Organizations. The Compliance Audits shall be a WebTrust for Certification Authorities or an equivalent audit standard approved by OpenPEPPOL which includes: A Report of Policies and Procedures in Operation and Test of Operational Effectiveness.

8.5 Actions Taken as a Result of Deficiency

After receiving a Compliance Audit report, the audited entity discusses with OpenPEPPOL any exceptions or deficiencies shown by the Compliance Audit. OpenPEPPOL shall also be entitled to discuss such exceptions or deficiencies with the audited party. The audited entity and OpenPEPPOL shall, in good faith, use commercially reasonable efforts to agree on a corrective action plan for correcting the problems causing the exceptions or deficiencies and to implement the plan.

8.6 Communication of Results

Following any Compliance Audit, the audited entity shall provide the OpenPEPPOL Transport Infrastructure Coordinating Community with the annual report and attestations based on its audit or self-audit within fourteen (14) days after the completion of the audit and no later than forty-five (45) days after the anniversary date of commencement of operations.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

OpenPEPPOL will not charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The PKI Service Provider shall maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

9.2.2 Other Assets

The PKI Service Provider shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers shall, subject to Section 9.3.2, be kept confidential and private ("Confidential/Private Information"):

- Certificate Application records,
- Transactional records (both full records and the audit trail of transactions),
- PTN audit trail records created or retained by OpenPEPPOL or the PKI Service Provider or and RA organization
- PTN audit reports created by OpenPEPPOL, the PKI Service Provider, or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of OpenPEPPOL/the PKI Service Provider and RA organization hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

OpenPEPPOL acknowledges that Certificates, Certificate revocation and other status information, repositories of the PTN, and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

Upon receiving private information the PTN CA and RAs shall secure it from compromise and disclosure to third parties.

9.4 Privacy of Subscriber Information

OpenPEPPOL does not process personal information.

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private.

9.4.3 Information Not Deemed Private

Subject to Belgian law, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

Upon receiving private information the PTN CA and RAs shall secure it from compromise and disclosure to third parties and shall comply with Belgian law in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CP, private information will not be used without the consent of the party to whom that information applies. This section is subject to applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

OpenPEPPOL shall be entitled to disclose Confidential/Private Information if, in good faith, OpenPEPPOL believes that:

- Disclosure is necessary in response to subpoenas and search warrants.
- Disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

No stipulation

9.5 Intellectual Property Rights

The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

OpenPEPPOL retains all Intellectual Property Rights in and to the Certificates and revocation information that their CAs issue.

OpenPEPPOL shall grant permission to use revocation information to perform Relying Party functions.

9.5.2 Property Rights in the CP

No stipulation.

9.5.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

The PTN Root and Issuing CAs own their public keys and certificates and all key generation materials. The end entity Subscriber organizations own their private keys.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

PTN CAs that issue certificates that assert a policy OID defined in this document warrant that:

- Their Certificates meet all material requirements of this CP and the applicable CPS, and
- Revocation services and use of a repository conform to all material requirements of this CP and the applicable CPS in all material aspects.
- Registration information is accepted only from RAs who accept the terms of the RA Agreement which includes their obligation to comply with this policy

9.6.2 RA Representations and Warranties

PTN RAs that perform registration functions described in this policy warrant that:

- Their registration functions are performed in accordance with a CPS approved by OpenPEPPOL for use with this policy,
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
- It is ensured that the organization applying for a certificate has signed the OpenPEPPOL AP or SMP Provider Agreement ([APA] or [SMPA]) before the application is approved.

Subscriber Agreements may include additional representations and warranties

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CP and the applicable CPS and the provider agreement established with OpenPEPPOL,
- Notify the CA in a timely manner of suspicion that their private keys are compromised or lost, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, Subscriber Agreements shall disclaim OpenPEPPOL possible warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8 Limitations of Liability

Under no circumstances will the OpenPEPPOL CAs be liable to any purported Relying Parties, or any other person or entity, for any loss of use, revenue or profit, lost or damaged data, or other commercial or economic loss or for any other direct, indirect, incidental, special, punitive, exemplary or consequential damages whatsoever, even if advised of the possibility of such damages or if such damages are

foreseeable. This limitation shall apply even in the event of a fundamental breach or a breach of the fundamental terms of this policy.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

Indemnifications are established by relevant OpenPEPPOL agreements.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law shall Relying Parties be required to indemnify OpenPEPPOL and the PKI Provider or RA organizations for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

9.10 Term and Termination

9.10.1 Term

The CP becomes effective upon publication in the OpenPEPPOL repository. Amendments to this CP become effective upon publication in the OpenPEPPOL repository.

9.10.2 Termination

This CP as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CP, PTN participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

All parties shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this CP may be made by the OpenPEPPOL Transport Infrastructure Coordinating Community. Amendments shall either be in the form of a document containing an amended form of the CP or an update. Amended versions or updates shall be published at: **https://www.peppol.eu/** Updates supersede any designated or conflicting provisions of the referenced version of the CP. The OpenPEPPOL Transport Infrastructure Coordinating Community shall determine whether changes to the CP necessitates a change in the corresponding Certificate Policy object identifier.

9.12.2 Notification Mechanism and Period

The OpenPEPPOL Transport Infrastructure Coordinating Community reserves the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The OpenPEPPOL Coordinating Authority's decision to designate amendments as material or non-material shall be within the OpenPEPPOL Coordinating Authority's sole discretion

Proposed amendments to the CP shall also be published at: **https://www.peppol.eu/**

The OpenPEPPOL Transport Infrastructure Coordinating Community solicits proposed amendments to the CP from the PKI provider or the RA organizations. If the OpenPEPPOL Transport Infrastructure Coordinating Community considers such an amendment desirable and proposes to implement the amendment, the OpenPEPPOL Transport Infrastructure Coordinating Community shall provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CP to the contrary, if the OpenPEPPOL Transport Infrastructure Coordinating Community believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of the PTN or any portion of it, OpenPEPPOL and the Transport Infrastructure Coordinating Community shall be entitled to make such amendments by publication in the OpenPEPPOL Repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, OpenPEPPOL shall provide notice of such amendments.

9.12.2.1 Comment Period

No stipulation.

9.12.2.2 Mechanism to Handle Comments

No stipulation.

9.12.3 Circumstances under Which OID must be Changed

If the OpenPEPPOL Transport Infrastructure Coordinating Community determines that a change is necessary in the object identifier corresponding to the Certificate policy, the amendment shall contain the new object identifier for the Certificate policy corresponding to OpenPEPPOL Certificates.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among OpenPEPPOL, Service Providers or Relying Parties

Disputes among one or more of any of OpenPEPPOL, Service Providers and/or Pelying Parties shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, Subscriber Agreements shall contain a dispute resolution clause.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of the Belgium shall govern the enforceability, construction, interpretation, and validity of this CP. This choice of law is made to ensure uniform procedures and interpretation for all PTN Participants, no matter where they are located.

This governing law provision applies only to this CP. Agreements incorporating the CP by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability,

construction, interpretation, and validity of the terms of the CP separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

This CP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.15 Compliance with Applicable Law

This CP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

In the event that a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP shall remain valid.

9.16.4 Enforcement (Attorney Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements shall include a force majeure clause protecting OpenPEPPOL and its service providers.

9.17 Other Provisions

No stipulation.

10 APPENDIX A: DEFINITIONS

access	Ability to make use of any information system (IS) resource.
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
archive	Long-term, physically separate storage.

Attribute Authority	An entity, recognized by a CMA, as having the authority to verify the association of attributes to an identity.
audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
audit data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
authenticate	To confirm the identity of an entity when that identity is presented.
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
backup	Copy of files and programs made to facilitate recovery if necessary.
binding	Process of associating two related elements of information.
biometric	A physical or behavioral characteristic of a person.
certificate	A digital representation of information which at least (1) identifies the CA issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the CA issuing it. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates.
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
certificate-related information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by NIST
confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
cryptoperiod	Time span during which each key setting remains in effect.
data integrity	Assurance that the data are unchanged from creation to reception
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services

erroneous issuance	Issuance of a certificate not materially in accordance with the procedures required by the CPS, issuance of a certificate to a person other that the one named as the subject of the certificate, or issuance of a certificate without the authorization of the person named as the subject of such certificate.
firewall	Gateway that limits access between networks in accordance with local security policy.
impersonation	Requesting and being issued a certificate issued under this CPS based on false or falsified information relating to naming or identity.
integrity	Protection against unauthorized modification or destruction of information.
intellectual property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
key escrow	The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Local Registration Authority (LRA)	An RA with responsibility for a local community.
naming authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization; the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI OIDs are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties using a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
PKI Sponsor	Fills the role of a Subscriber on behalf of an organizational role or organizations that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this document.
Policy Authority (PA)	Authority that oversees the creation and update of Certificate Policies, reviews Certification Practice Statements, reviews the results of CA audits for policy compliance, evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies.
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Private key compromise	A loss, theft or modification, or unauthorized access of a private key corresponding to the public key listed in a certificate governed by this CPS, including without limitation by cryptographic analysis or key extraction.
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.

Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates.
revocation	The act or process of prematurely ending the operational period of a certificate effective at a specific date and time.
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
server	A system entity that provides a service in response to requests from clients.
Signature certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions. Also referred to as an Identity Certificate.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. Current subscribers possess valid CDS-issued certificates.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (see subordinate CA)
system equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
trust list	Collection of Trusted Certificates used by Relying Parties to authenticate other certificates.
tier	A barrier such as a locked door or closed gate that provides mandatory access control for individuals and requires a positive response (e.g., door unlocks or gate opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access. Moreover, each physical security tier encapsulates the next inner tier, such that an inner tier must be fully contained in an outside tier and cannot have a common outside wall with the outside tier, the outermost tier being the outside wall of the building.
Trusted Agent	Entity authorized to act as a representative of a Certificate Management Authority in providing Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure, authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a "trust anchor".

Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
unauthorized revocation	Revocation of a certificate without the authorization of the subscriber.
zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

11 APPENDIX B: ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
CA	Certification Authority
CMA	Certificate Management Authority
CMS	Cryptographic Message Syntax
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSOR	Computer Security Objects Registry
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDSA	Elliptic curve Digital Signature Algorithm
I&A	Identification and Authentication
ID	Identity (also, a credential asserting an identity)
ISO	International Organization for Standards
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
POC	Point of Contact
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption and digital signature algorithm)
S/MIME	Secure Multipurpose Internet Mail Extensions
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
TA	Trusted Agent
TLS	Transport Layer Security
USC	United States Code
USD	United States Dollar

12 APPENDIX C: REFERENCES

The following documents contain information that provides background, examples, or details about the contents of this policy.

Number	Title	Date
ABADSG	Digital Signature Guidelines http://www.abanet.org/scitech/ec/isc/dsgfree.html	1 August 1996
APA	"PEPPOL Transport Infrastructure Agreements - AP Provider Agreement", Version 3.0.	June 2012
BUSDOX	Secure Trusted Asynchronous Reliable Transport (START), Version 1.0". Lightweight Message Exchange Profile (LIME), Version 1.0" Service Metadata Locator Profile: Physical interfaces and bindings for the Service Metadata Locator Service, Version 1." "Service Metadata Publishing, Version 1.0"	December 2009
FIPS140	Security Requirements for Cryptographic Modules http://csrc.nist.gov/publications/index.html	21 May 2001
FIPS112	Password Usage http://csrc.nist.gov/	5 May 1985
FIPS186-3	Digital Signature Standard http://csrc.nist.gov/publications/drafts/fips_186-3/Draft_FIPS-186-3%20_November2008.pdf	March 2006
FOIAACT	5 U.S.C. 552, Freedom of Information Act http://www4.law.cornell.edu/uscode/5/552.html	
NS4009	NSTISSI 4009, National Information Systems Security Glossary	January 1999
PCA	"PEPPOL Transport Infrastructure Agreements – Authority Agreement", Version 3.0.	June 2012
PKCS-1	PKCS #1 v2.0: RSA Cryptography Standard http://www.rsa.com	1 October 1998
PKCS-12	Personal Information Exchange Syntax Standard http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html	April 1997
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP http://www.ietf.org/rfc/rfc2560.txt?number=2560	June 1999
RFC3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford. *http://www*.ietf.org/rfc/rfc2527.txt	November 2003
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	May 2008
SMPA	"PEPPOL Transport Infrastructure Agreements - SMP Provider Agreement", Version 3.0	June 2012