Version: 7.0
Document date: 16.11.2020
Effective date: 01.12.2020

PUBLIC

# Certification Practice Statement

## Buypass Class 3 Enterprise Certificates

Buypass AS, Nydalsveien 30A, PO box 4364 Nydalen, 0402 Oslo

www.buypass.no | 22 70 13 00

**TABLE OF CONTENTS**

# 1 Introduction

## 1.1 Overview

A Certificate Policy (CP) is a “named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements"[1].

A Certification Practice Statement (CPS) is a “statement of the practices which a Certificate Authority employs in issuing Certificates” [1].

This document contains the Certificate Policy and Certification Practice Statement for Buypass Class 3 Enterprise Certificates provided as Soft Token or Hard Token.

Buypass is the Certificate Authority (CA) for all Buypass Class 3 Enterprise Certificates.

A Class 3 Enterprise Certificate Subscriber SHALL be an organization that is registered in a QGR.

For the purpose of this document, a Subscriber denotes the organization who contracts with the CA for the issuance of Certificates. For Key/Certificate management operations the Subscriber shall be represented by human persons in the role of Authorized Subscriber Representatives.

The Subject denotes a non-human entity (application or system) that represents the Subscriber and which is the holder of the Private Key associated with the Public Key to which the Certificate is issued. The Subject shall be represented by a person in the role of a Subject Sponsor who undertakes the Subject’s obligations as defined in the Certificate Policy for Buypass Enterprise Certificates [20].

Certificates issued under this policy are compliant with “*Virksomhetssertifikater*” according to ‘Kravspesifikasjon for PKI i offentlig sector’ [23]. The Certificate Policy for Buypass Class 3 Enterprise Certificates [20] is aligned with the Normalized Certificate Policy (NCP [16]) for Soft Tokens and the extended Normalized Certificate Policy (NCP+ [16]) for Hard Tokens.

The Certificates may also be EU Qualified Certificates issued to legal persons according to Regulation (EU) No 910/2014 [22]. The Certificate Policy for Buypass Class 3 Enterprise Certificates [20] is in this case aligned with the Qualified Certificate Policy for legal persons (QCP-l [17]) for both Hard Tokens and Soft Tokens.

The EU Qualified Certificates may also meet the regulatory requirements for PSD2 [29] and the Regulatory Technical Standard (RTS) [30]. The Certificate Policy for Buypass Class 3 Enterprise Certificates [20] is in this case aligned with the Qualified Certificate Policy for legal persons (QCP-l [17]) with additional policy requirements from ETSI TS 119 495[14].

### 1.1.1 CA hierarchy

The CPS shall include the complete CA hierarchy, including root and subordinate CAs.

The CA hierarchies used for Buypass Class 3 Enterprise Certificates comprises three different hierarchies:

1. The Buypass Class 3 CA hierarchy,
2. The Buypass Class 3 G2 HT CA hierarchy and
3. The Buypass Class 3 G2 ST CA hierarchy

The Buypass Class 3 CA hierarchy consists of the Buypass Class 3 Root CA and the two issuing CAs Buypass Class 3 CA 2 and Buypass Class 3 CA 3.

Buypass Class 3 CA 2 issues Buypass Class 3 SSL certificates while Buypass Class 3 CA 3 issues Enterprise Certificates as specified in this document and Qualified Certificates for natural persons.

The Buypass Class 3 G2 HT CA hierarchy consist of the Buypass Class 3 Root CA G2 HT and the two issuing CAs Buypass Class 3 CA G2 HT Person and Buypass Class 3 CA G2 HT Business.

Buypass Class 3 CA G2 HT Person issues Qualified Certificates to natural persons while Buypass Class 3 CA G2 HT Business issues Enterprise Certificates as specified in this document.

The Buypass Class 3 G2 ST CA hierarchy consist of the Buypass Class 3 Root CA G2 ST and Buypass Class 3 CA G2 ST Business.

Buypass Class 3 CA G2 ST Business issues Enterprise Certificates as specified in this document.

## 1.2 Document name and Identification

The Class 3 Enterprise Certificate Policy covered by this document has been provided the following Buypass Certificate Policy Identifiers / OIDs;

- OID 2.16.578.1.26.1.3.2 – provided as Soft Token
- OID 2.16.578.1.26.1.3.5 – provided as Hard token

EU Qualified Certificates issued under this policy also include the following OID

- OID 0.4.0.194112.1.1 (ETSI QCP-l)

Relying Parties SHALL recognize a particular Certificate as having been issued under [20] by inspecting the Certificate Policies extension field of the Certificate, which then shall hold one of the policy OIDs above.

Buypass Class 3 CA 3 also issues Qualified Certificates to natural persons under the following Buypass Certificate Policies / OIDs:

- OID=2.16.578.1.26.1.3.1 – the private keys are protected in a smart card
- OID=2.16.578.1.26.1.3.6 – the private keys are protected in an HSM

### 1.2.1 Revisions

| Version | Document Date | Description/Change |
|---|---|---|
| 1.1 | 07.11.2008 | Approved by Buypass Policy Board. |
| 1.2 | 18.06.2009 | Included new roles Certificate manager and Partner. Approved by Buypass Policy Board. |
| 1.3 | 19.02.2010 | Approved by Buypass Policy Board. Minor changes. |
| 1.4 | 27.05.2010 | Approved by Buypass Policy Board. Changes regarding use of Social Security Number and new version of Hvitvaskingsforskriften. |

| Version | Document Date | Description/Change |
|---|---|---|
| 1.5 | 30.09.2010 | Approved by Buypass Policy Board. Updated with logging and new CA structure. |
| 1.6 | 20.01.2011 | Approved by Buypass Policy Board. Minor changes. |
| 1.7 | 29.04.2011 | Approved by Buypass Policy Board. Minor changes. |
| 1.8 | 13.01.2012 | Approved by Buypass Policy Board. Minor changes. |
| 1.9 | 01.06.2012 | Approved by Buypass Policy Board. Minor changes. |
| 2.0 | 11.05.2013 | Added Enterprise certificates provided as hard tokens. Compliance Audit changed from WebTrust to ETSI. |
| 3.0 | 12.10.2015 | General revision. Added Distribution Key sent by SMS as an option when ordered by pre-authorized and electronically authenticated Certificate Applicant. |
| 4.0 | 16.06.2017 | Adapted to ETSI EN 319 411-1/2 and EN 319 401. Included Certificates based on Subscriber generated keys. Included Qualified Certificates for electronic Seals according to eIDAS. |
| 5.0 | 31.05.2018 | Converted to RFC 3647 format. |
| 5.1 | 31.10.2018 | Included European Business Register. |
| 6.0 | 03.06.2019 | Included PSD2 Qualified Certificates for electronic Seals – according to ETSI TS 119 495, added some more specific eIDAS requirements and changed procedures for CP/CPS notifications. |
| 7.0 | 16.11.2020 | Included generation 2 (G2) of root CAs and issuing CAs. |

## 1.3 PKI Participants

This document is intended for Registration Authorities, Subscribers, Relying Parties and Subcontractors.

### 1.3.1 Certification Authorities

Buypass is the Certificate Authority (CA) for all Buypass Class 3 Enterprise Certificates.

### 1.3.2 Registration Authorities

Buypass is the main Registration Authority (RA) for all Buypass Class 3 Enterprise Certificates.

A Distribution Service Provider may be used to verify the identity of an authorised representative of the Subscriber by physical presence at time of delivery. Other service providers may also be used to verify the identity remotely e.g. by electronic identification means, using qualified electronic signatures etc (e.g. eID providers, QTSPs) etc.

### 1.3.3 Subscribers

A Subscriber under this policy MUST be a legal person registered in a QGR. A Subject under this policy MAY be an application or system that represents, and operates on behalf of the Subscriber.

### 1.3.4 Relying Parties

### 1.3.5 Other Participants

## 1.4 Certificate Usage

Buypass Class 3 Enterprise Certificates is applicable for supporting PKI based security services between organizations (private and governmental) as well as between organizations and private consumers. In particular, the Certificates can be used to:

- authenticate the identity of an organization
- encrypt data for an organization or to exchange symmetric keys to be used for encryption
- verify organizational electronic signatures or electronic seals

### 1.4.1 Primary Certificate Purposes

### 1.4.2 Secondary Certificate Purposes

### 1.4.3 Excluded Certificate Purposes

Buypass Class 3 Enterprise Certificates SHALL NOT be used

- to sign software, certificates and/or revocation lists
- for web-based data communication conduits via TLS/SSL protocols, for this purpose SSL certificates should be used
- as a basis for issuing other certificates, electronic IDs or credentials unless explicitly agreed upon by Buypass

## 1.5 Policy administration

### 1.5.1 Organization Administering the Document

Buypass Policy Board is responsible for the Certificate Policy [20] and Certification Practice Statement [21] and their maintenance.

### 1.5.2 Contact Person

Contact point for questions regarding the Certificate Policy [20] and Certification Practice Statement [21] is:

Buypass Policy Board
c/o Buypass AS
P.O Box 4364 Nydalen
N-0402 Oslo

Telephone: + 47 22 70 13 00
Email: policy@buypass.no

### 1.5.3 Person Determining CPS suitability for the policy

### 1.5.4 CPS approval procedures

A defined review process should exist to ensure that the CP is supported by the CA's CPS.

The Certification Practice Statement [21] is approved by Buypass Policy Board. All document changes must be formally approved by Buypass Policy Board.

## 1.6 Definitions and acronyms

### 1.6.1 Definitions

| Terms | Definition |
|---|---|
| Activation Data | Data that gives access to the Private key |
| Anti-money laundering (AML) | AML refers to a set of laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income. |
| Authoritative Source | Any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity. |
| Authorization Code | Secret code used to ensure physical presence of Authorised Subscriber Representative in case of Subscriber generated Private Key. |
| Authorization Number | A unique identifier of a Payment Service Provider acting as the Subscriber for PSD2 Certificates. The Authorization Number is used and recognized by the NCA. |
| Authorized Officer | Authorized Subscriber Representative who has authority on behalf of Subscriber to confirm the identity of the Subscriber by physical presence according to article 24 of the Regulation (EU) No 910/2014 [22]. The Contract Signer may act as Authorized Officer. |

| Terms | Definition |
|---|---|
| Authorized Subscriber Representative | A natural person who has express authority to represent the Subscriber. |
| Buypass | Buypass AS, registered in the Central Coordinating Register for Legal Entities with organization number 983 163 327. |
| Buypass Certification Services | CA Services as described in this Policy. Encompasses the following services:<br>Registration service: verifies the identity of and, if applicable, any specific attributes of a Subject. The results of this service are passed to the certificate generation service. This can include key generation.<br>Certificate generation service: creates and signs certificates based on the identity and other attributes verified by the registration service.<br>Dissemination service: disseminates certificates to Subjects, and if the Subject consents, makes them available to relying parties. This service also makes available the CA's terms and conditions and any published policy and practice information, to Subscribers and Relying Parties.<br>Revocation management service: processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.<br>Revocation status service: provides certificate revocation status information to relying parties.<br>Subject device provision service: prepares, and provides or makes available secure cryptographic devices, or other secure devices to Subjects. |
| Buypass Policy Board | The Board responsible for all Certificate Policies in Buypass. |
| Buypass Web | Websites operated by Buypass, i.e. www.buypass.no and www.buypass.com. |
| Central Coordinating Register for Legal Entities | Norwegian national register containing basic data (e.g. Organization Name and Organization Number) about legal entities to coordinate information on business and industry that resides in various public registers (“Enhetsregisteret”). |
| Certificate | An electronic document that uses a digital signature to bind a public key and an identity. In this document the term is used synonymously with Buypass Class 3 Enterprise Certificate. |
| Certificate Applicant | Authorized Subscriber Representative who has privileges to submit a Certificate application on behalf of the Subscriber. |
| Certificate Application Authority | Authorization on behalf of the Subscriber to submit a Class 3 Enterprise Certificate application on behalf of Subscriber, provide the information requested from Subscriber by the CA for issuance of the Class 3 Enterprise Certificate and authorize a person to operate in a Subject Sponsor role representing the Subscriber. |
| Certificate Authority (CA) | An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs. |
| Certificate Manager | Authorized Subscriber Representative who has the authority to (i) act as a Certificate Applicant and (ii) to authorize other employees or third parties to act as a Certificate Applicant. |
| Certificate Policy (CP) | A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements. |

| Terms | Definition |
|---|---|
| Certificate Rekey | The issuance of a new Certificate for a previously registered Subscriber based on a new key pair. This includes routine rekey, rekey prior to expiration and rekey after revocation. |
| Certification Practice Statement (CPS) | Statement of the practices which a Certificate Authority employs in issuing Certificates (see [1]). |
| Contract Signer | Authorized Subscriber Representative who has authority on behalf of Subscriber to sign Subscriber Agreements. |
| Distribution Key | Secret key that protects access to CA generated Subject Private keys during Soft Token distribution from CA to Subject Sponsor. |
| Distribution Service Provider | Entity or a legal person who provides services for distributing physical or electronic objects to Subjects. The services may include authentication of the receiver based on physical presence or using other electronic identification providing equivalent assurance to physical presence. |
| Electronic Seal | Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity (see Regulation (EU) No 910/2014 [22]). |
| Electronic Signature | Data in electronic form which are attached to or logically associated with other electronic data and which is used by the signatory to sign (see Regulation (EU) No 910/2014 [22]). |
| European Business Register (EBR) | The European Business Register (EBR) is a network of National Business Registers and Information Providers in European Countries containing basic data (e.g. Organization name and Organization Number) about legal entities operating in these countries. EBR includes the Norwegian Central Coordinating Register for Legal Entities ("Enhetsregisteret"). |
| Hard Token | A secure user device protecting the Private Keys. In this document the Hard Token is a smart card if Buypass generates the Private Key and an HSM if the Subscriber generates the Private Key. |
| Hardware Security Module (HSM) | A secure cryptographic module used to generate, store and handle cryptographic keys. The HSM provides logical and physical protection of the keys. |
| High Security Zone | An area (physical or logical) protected by physical and logical controls that protects a CA's Private Key and cryptographic hardware. |
| National Competent Authority (NCA) | A national authority responsible for payment services. The NCA approves or rejects authorizations for Payment Service Providers in its country. |
| Organization Number | Unique registration number identifying a legal person. Assigned by a national authority in the jurisdiction where the legal person operates. |
| Partner | A legal person given the authority to assign natural persons as Authorized Subscriber Representatives on behalf of one or more Subscribers through the initial Subscriber Registration.<br>The legal person must have signed a Contractual agreement with Buypass before acting as a Partner. |
| Personal Identification Number | A unique identifier for natural persons as defined in an Authoritative Source. |
| Payment Service Directive 2 (PSD2) | Directive (EU) 2015/2366 [29] |
| Payment Service Provider (PSP) | An organization authorised to provide payment services to customers. |
| Private Key | The key of a key pair that is kept secret by the holder of the key pair, and that is used to create Digital Signatures and/or to decrypt |

| Terms | Definition |
|---|---|
| | electronic records or files that were encrypted with the corresponding Public Key. |
| Public Key | The key of a key pair that MAY be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key. |
| PSD2 Certificate | EU Qualified Certificate meeting regulatory requirements for PSD2 [29] and the Regulatory Technical Standard (RTS) [30]. |
| Qualified Certificate | A certificate for electronic seals, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of the Regulation (EU) No 910/2014 [22] |
| Qualified Government Register (QGR) | Any Authoritative Source provided by a Government Entity containing basic information about legal persons operating in the Government's jurisdiction. The basic information includes the full name of the legal person, a nationally recognized registration number and a business and/or postal address for the legal person. All registers in EBR are QGRs. QGRs hold information about legal persons as required by national legislation. |
| Relying Party | Recipient of a Certificate which acts in reliance on that Certificate and/or digital signatures verified using that Certificate (see [1]) |
| Signing Authority | Authorization to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Subscriber. |
| Signing Authority Statement | A statement that expressly documents a person's Signing Authority. |
| Soft Token | If Buypass generates the Private Key, this is an encrypted file protecting the Private Keys during distribution from the CA to the Subject Sponsor. The file is a PKCS#12 file encrypted with a Distribution Key. If the Subscriber generates the Private Key, this represents a key store controlled by the Subscriber. |
| Subcontractor | Party providing services on behalf of the CA. |
| Subject | Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate |
| Subject Key Provision Service | Prepares and provides cryptographic keys in a secure user device (Hard Token or Soft Token) to subjects. |
| Subject Information | Attributes that describe the Subject |
| Subject Sponsor | Authorized Subscriber Representative who has privileges to undertake the Subject's obligations under this policy whenever the Subject is a non-human entity. |
| Subscriber | A legal person to whom a Certificate is issued and who is legally bound by a Subscriber Agreement |
| Subscriber Agreement | An agreement between the CA and the Subscriber that specifies the rights and responsibilities of the parties under this policy. |

### 1.6.2 References

[1] IETF RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practises Framework – 2003
[2] IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008
[3] Policy for sikkerhet og kvalitet i Buypass
[4] FIPS PUB 140-1: "Security Requirements for Cryptographic Modules"
[5] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules"

[6] SEID prosjektet leveranse oppgave 1 Anbefalte Sertifikatprofiler for personsertifikater og virksomhetssertifikater, versjon 1.01
[7] ETSI EN 319 412-3 – Certificate Profiles: Part 3: Certificate profile for certificates issued to legal persons
[8] ETSI EN 319 412-5 – Certificate Profiles: Part 5: QC Statements
[9] ISO/IEC 9594-8 Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
[10] ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
[11] ISO/IEC 27002:2013 Information technology - Security techniques. Code of Practice for Information Security Management
[12] ISO/IEC 15408 (parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security"
[13] ETSI TS 119 312 – Cryptographic Suites
[14] ETSI TS 119 495 - Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
[15] ETSI EN 319 401 – General policy requirements for Trust Service Providers
[16] ETSI EN 319 411-1 – Policy and security requirements for Trust Service Providers issuing certificates; Part 1 General requirements
[17] ETSI EN 319 411-2 – Policy and security requirements for Trust Service Providers issuing certificates; Part 2 Requirements for Trust Service Providers issuing EU Qualified Certificates
[18] IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP), June 2014
[19] Buypass Class 3 Certificate and CRL profiles, current version
[20] Certificate Policy for Buypass Class 3 Enterprise Certificates, current version, included in this document.
[21] Certification Practice Statement for Buypass Class 3 Enterprise Certificates, this document
[22] Regulation (EU) No 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[23] Kravspesifikasjon for PKI i offentlig sektor, Versjon 2.0 Juni 2010
[24] Forskrift om frivillige selvdeklarasjonsordninger av 21. november 2005 nr. 1296
[25] FOR-2018-09-14-1324 Hvitvaskingsforskriften. «Forskrift om tiltak mot hvitvasking og terrorfinansiering»
[26] CEN Workshop Agreement 14171: “General guidelines for electronic signature verification”.
[27] Lov 15.juni 2018 nr 38 om behandling av personopplysninger (personopplysningsloven)
[28] Forskrift 15.juni 2018 nr 875 om behandling av personopplysninger (personopplysningsforskriften)
[29] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
[30] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Text with EEA relevance).

### 1.6.3 Conventions

Text that is outside text boxes is the Certificate Policy [20]. All Certificate Policy requirements contain either a SHALL, SHALL NOT, SHOULD, SHOULD NOT or MAY statement.

Text contained inside blue coloured text boxes are Certification Practice Statement related and specifies in more detail the practices employed by Buypass to meet the requirements of the Certificate Policy.

Most Certificate Policy requirements concerning either the CA or RA services provided by Buypass have a CPS text box related to them. A CA or RA related Certificate Policy requirement may not have a corresponding CPS text box if it considered self explanatory how the requirement is fulfilled.

Hereinafter the term Certificate is used synonymously with Buypass Class 3 Enterprise Certificates.

# 2 Publication and repository responsibilities

## 2.1 Publication of information

a) The Certificate Policy for Buypass Class 3 Enterprise Certificates [20] and the Certification Practice Statement for Buypass Class 3 Enterprise Certificates [21] SHALL be publicly available on the Buypass Web 24x7.

The Certificate Policy for Buypass Class 3 Enterprise Certificates [20] and the Certification Practice Statement for Buypass Class 3 Enterprise Certificates [21] are available 24x7 and accessible on Buypass Web.

b) Revocation status information SHALL be publicly available at the location(s) specified in the appropriate extensions of every Certificate issued.

Every Class 3 Enterprise Certificate issued by Buypass contains a CRL distribution point extension that contains a URL for CRL retrieval and an Authority Information Access extension that contains a URL for OCSP service access. Both Certificate revocation status services are available 24x7 and accessible on Buypass Web.

The CRL may also be available through the LDAP protocol using the URL included in the CRL Distribution Point extension. The LDAP service is available 24x7 and accessible on Buypass Web.

c) Buypass Class 3 Enterprise Certificates SHALL be publicly available for Subscribers and Relaying Parties.

All Certificates are available through the LDAP protocol. The LDAP service is available 24x7 and accessible on Buypass Web.

d) Buypass Class 3 Enterprise Certificates SHALL be available for retrieval in only those cases for which the Subscriber's consent has been obtained.

The Subscriber must accept that the certificate is published as a prerequisite when applying for an Enterprise certificate

## 2.2 Time or frequency of publication

## 2.3 Access controls on repositories

# 3 Identification and authentication

## 3.1 Naming

### 3.1.1 Types of names

### 3.1.2 Need for names to be meaningful

### 3.1.3 Anonymity or pseudonymity of subscribers

### 3.1.4 Rules for interpreting various name forms

### 3.1.5 Uniqueness of names

### 3.1.6 Recognition, authentication, and role of trademarks

## 3.2 Initial identity validation

### 3.2.1 Method to Prove Possession of Private Key

a) If the Subject's key pair is generated by the Subscriber, the Certificate request process SHALL ensure that the Subscriber has possession of the Private Key associated with the Public Key presented for certification.

Buypass verifies the signature on every PKCS#10 Certificate Signing Request using the public key submitted for certification. If the signature is valid, Buypass knows that the signature was generated using the corresponding Private Key.

b) If the proof of possession validation fails during CAs verification of a Certificate request, the Certificate SHALL NOT be issued and the Certificate Applicant SHALL be notified without undue delay.

If Certificate Signing Request signature verification fails, the Certificate Application is rejected and the Certificate Applicant is notified immediately.

### 3.2.2 Authentication of Organization Identity

The following Subscriber information SHALL be presented to the RA during initial registration:

- full name and legal status of the Subscriber as defined in a QGR
- the Subscriber's Organization Number as defined in a QGR
- name and contact information of all Subscriber representatives authorized to operate as either Certificate Manager, Certificate Applicant, Subject Sponsor, Authorized Officer or Contract Signer

As part of initial Subscriber Registration, it is mandatory that the Subscriber register the following information with Buypass using a web based registration procedure:

- the Subscriber Organization Name and Organization Number as registered in a QGR
- the address of Subscriber place of business as registered in a QGR
- name, job title or date of birth and contact information for a Contract Signer
- in case of EU Qualified Certificates, name, date of birth or job title and contact information for an Authorized Officer

The Subscriber must also register the following information for at least one person, acting as either Certificate Manager, Certificate Applicant or Subject Sponsor:

- name, Personal Identification Number and contact information for a Certificate Manager
- name, job title or date of birth or Personal Identification Number and contact information for a Certificate Applicant or
- a Partner's Organization Name and Organization Number as registered in a QGR, in case the Partner is authorized to act as the Certificate Applicant on behalf of the Subscriber
- name and contact information of the Subject Sponsor

The Partner will register Name, Personal Identification Number and contact information of the natural persons authorized to act as Certificate Applicants on behalf of the Partner

All information registered is incorporated into a Subscriber Agreement that is signed and thereby confirmed by the Contract Signer.

If the Subscriber later on wants to add, remove or change registered Subscriber information, the Subscriber needs to go through a new "Subscriber Registration and Subscriber Agreement Signing" step (see 4.1.1). An

exception is the following changes that may be performed without going through a new "Subscriber Registration and Subscriber Agreement Signing" step:

- the Contract Signer and Certificate Manager may change information about authorized Certificate Applicants

3.2.2.1 Amendments for PSD2 certificates

a) In case of EU Qualified Certificates for PSD2, the CA SHALL verify the PSD2 specific attributes (PSD2 Authorization Number or other recognized identifier, roles, name of the NCA) provided by the Subscriber using authentic information from the NCA (e.g. a national public register, EBA PSD2 Register, EBA Credit Institution Register, authenticated letter).

Buypass verifies the PSD2 specific attributes either directly against an NCA, or against an NCA register or the EBA register. This is done for the Authorization Number and the PSP Roles.

The PSD2 Authorization Number is verified to represent the same legal person as identified in section 3.2.2.

b) If the NCA provides rules for validation of these attributes, the CA SHALL apply the given rules.

Buypass adapts the validation rules according to NCA specifications on demand.

## 3.2.3 Authentication of Individual Identity

The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:
i) by the physical presence of an authorized representative of the legal person; or
ii) using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which the CA can prove the equivalence.

In case of EU Qualified Certificates, the Authorized Officer acts as the authorized representative for the legal person. Otherwise, any of the other Authorized Subscriber Representatives may represent the legal person.

Before a new Certificate is disseminated to either a Subscriber, Subject or any Relying Party at least one Authorized Subscriber Representative involved in the certification process (Authorized Officer, Certificate Applicant or Subject Sponsor) SHALL be authenticated, either by physical presence or remotely.

***a) Physical presence:*** The Authorized Subscriber Representative SHALL authenticate himself/herself

- in person towards an RA representative by presenting a nationally recognized identity document. Acceptable documents are documents compliant with the requirements stated in ”Hvitvaskingsforskriften, §4-3” [25] or similar AML legislation in other countries. The RA representative SHALL verify that the documents are acceptable and valid.

Commercial services provided by the Norwegian Postal Service are used to

i) provide personal delivery to the Subject Sponsor of either the Distribution Key for a Soft Token or the token itself for a Hard Token in case of CA generated private keys or

ii) provide personal delivery to the Certificate Applicant of an Authorization Code in case of Subscriber generated private keys.

iii) provide personal delivery to the Authorized Officer of an Authorization Code in case of EU Qualified Certificates.

Face-to-face authentication of the Authorized Subscriber Representative (Subject Sponsor, Certificate Applicant or Authorized Officer) is part of the personal delivery routine.

***b) Remotely:*** The Authorized Subscriber Representative SHALL authenticate himself/herself

- by using electronic identification means, for which prior to the issuance of the Certificate, a physical presence of the Authorized Subscriber Representative was ensured and which meets the requirements set out in Article 8 of Regulation (EU) No 910/2014 [22] with regard to the assurance levels 'substantial' or 'high'; or

An Authorized Subscriber Representative may use an electronic identification mean (eID) satisfying level of assurance 'high'. For Norway all eIDs at level 'high' are accepted. For other countries, notified eIDs at level 'high' are accepted and notified eIDs at level 'substantial' may be accepted.

- by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with Regulation (EU) No 910/2014 [22]); or

An Authorized Subscriber Representative may use a qualified electronic signature or qualified electronic seal according to Regulation (EU) No 910/2014 [22].

A Subscriber Agreement signed with a qualified electronic signature by a Contract Signer will be accepted as proof of identity for the Subscriber. In this case the Contract Signer acts as an Authorized Officer.

- by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence.

An Authorized Subscriber Representative may use an advanced electronic signature or advanced electronic seal based on qualified certificates according to Regulation (EU) No 910/2014 [22] if such signatures and seals are recognized at national level as providing similar assurance as physical presence.

In Norway advanced electronic signatures based on qualified certificates from Norwegian QTSPs are recognized at national level and accepted by Buypass. For other countries, an assessment against national law and accepted national practice will be performed before accepting advanced electronic signatures or seals.

A Subscriber Agreement signed with an advance electronic signature based on a qualified certificate from a Norwegian QTSP by a Contract Signer will be accepted as proof of identity for the Subscriber. In this case the Contract Signer acts as an Authorized Officer.

### 3.2.4 Non-verified Subscriber Information

### 3.2.5 Validation of Authority

The RA SHALL be able to identify both Certificate Managers, Certificate Applicants, Subject Sponsors, Authorized Officers and Contract Signers as Authorized Subscriber Representatives.

The same person MAY fill several of these roles at the same time.

a) A Contract Signer's Signing Authority SHALL be established through a Signing Authority Statement. Accepted Signing Authority Statements MAY be:
   - information obtained from a QGR identifying the Contract Signer as a person that has a defined role
   - an express authorization statement issued and signed by a person with Signing Authority according to a QGR

Buypass initially consults a QGR directly to verify whether the identified Contract Signer has a defined role in the QGR.

A signed statement from a person that is entitled to bind the Subscriber organization as defined above authorizing a person to act as a Contract Signer is accepted as well.

b) The Authorized Officer's authority to confirm the identity of the legal person SHALL be established through:

- a statement of Signing Authority as defined in a)
- an express authorization statement issued by an authorized Contract Signer

The Contract Signer may explicitly authorize the Authorized Officer through the signed Subscriber Agreement (either initial agreement or later amendments).

c) A Certificate Manager's Certificate Application Authority SHALL be established through:
- a statement of Signing Authority as defined in a)
- an express authorization statement issued by an authorized Contract Signer

The Contract Signer may explicitly authorize one or several Certificate Managers through the signed Subscriber Agreement (either initial agreement or later amendments). Buypass verifies the authenticity of the Authority Statement by contacting the Contract Signer.

The Contract Signer may authorize a Partner to act as a Certificate Manager. Buypass verifies the authenticity by contacting the Contract Signer. The Partner is authorized to assign natural persons to act as Certificate Managers on behalf of the Subscriber.

d) A Certificate Applicant's Certificate Application Authority SHALL be established through;
- a statement of Signing Authority as defined in a)
- an express authorization statement issued by an authorized Contract Signer or Certificate Manager

The Contract Signer explicitly authorizes the Certificate Applicant through the signed Subscriber Agreement. Buypass verifies the authenticity of the authorization by contacting the Contract Signer.

Buypass also accepts express authorization statements from an authorized Certificate Manager. Buypass verifies the authenticity of such authorization statement by contacting the Certificate Manager.

The Contract Signer may authorize a Partner to act as a Certificate Applicant. Buypass verifies the authenticity by contacting the Contract Signer. The Partner is authorized to assign natural persons to act as Certificate Applicants on behalf of the Subscriber.

e) Proof of authorization for a Subject Sponsor may be established either:
- through an Authorization Statement as for Certificate Applicants
- by having an already Authorized Certificate Applicant identify the Subject Sponsor in a Certificate Application

The Certificate Applicant explicitly identifies the Subject Sponsor through the Certificate Application.

f) The CA and Subscriber MAY enter into a written agreement, signed by a Contract Signer on behalf of Subscriber, whereby, for specified terms:
- Subscriber expressly authorize one or several Certificate Managers to exercise Certificate Application Authority and authority to authorize Certificate Applicants with respect to future Certificate Applications submitted on behalf of Subscriber
- Subscriber expressly authorizes one or several Certificate Applicants to exercise Certificate Application Authority with respect to future Certificate Applications submitted on behalf of Subscriber

As part of the Subscriber Registration process (see 4.1.1), the Subscriber enters into a Subscriber Agreement with Buypass. This Subscriber Agreement, signed by the Contract Signer, may expressly authorize:

- one or several Certificate Managers to authorize Certificate Applicants on behalf of the Subscriber
- one or several Certificate Managers and/or Certificate Applicants to exercise Certificate Application Authority with respect to future Certificate Applications submitted on behalf of Subscriber. In this case, the Subscriber Agreement provides that the Subscriber is obligated under the Subscriber Agreement for all

Certificate Applications issued by these Certificate Applicants until their Certificate Application Authority is revoked

### 3.2.6 Criteria for Interoperation or Certification

## 3.3 Identification and authentication for re-key requests

### 3.3.1 Identification and Authentication for Routine Re-key

The requirements for identification and authentication of Subscriber and Authorized Subscriber Representatives are the same as for initial registration (see 3.2).

The CA shall check the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the subject are still valid.

Subscriber information and authorizations already registered with Buypass may be reused during a renewal application.

If the Subscriber needs to make changes to any of the registered information before a renewal, the statements in 3.2.2 apply.

#### 3.3.1.1 Amendments for PSD2 Certificates

In case of EU Qualified Certificates for PSD2, the CA SHALL repeat the verification of the PSD2 specific attributes to be included in the certificate before certificate renewal.

PSD2 specific attributes are verified before certificate renewal – see 3.2.2.1.

### 3.3.2 Identification and Authentication for Re-key After Revocation

The requirements for identification and authentication of Subscriber and Authorized Subscriber Representatives are the same as for initial registration (see 3.2).

The CA SHALL check the existence of the certificate to be rekeyed and that the information used to verify the identity and attributes of the subject are still valid.

Subscriber information and authorizations already registered with Buypass may be reused during a rekey after revocation application.

If the Subscriber needs to make changes to any of the registered information before a rekey after revocation, the statements in 3.2.2 apply.

#### 3.3.2.1 Amendments for PSD2 Certificates

In case of EU Qualified Certificates for PSD2, the CA SHALL repeat the verification of the PSD2 specific attributes to be included in the certificate before certificate renewal.

PSD2 specific attributes are verified before certificate rekey after revocation – see 3.2.2.1.

## 3.4 Identification and authentication for revocation request

a) Only Authorized Subscriber Representatives MAY request Certificate revocation on behalf of the Subscriber.

Once a revocation request is received, Buypass will attempt to obtain an authenticated confirmation either by the Subscriber or from one of the Authorized Subscriber Representatives (Certificate Applicant, Certificate Manager, or a Contract Signer) already registered with Buypass for that particular Subscriber and Certificate.

b) The RA SHALL implement identification/authentication procedures that provide reasonable assurance that the requestor is an Authorized Subscriber Representative.

See 4.9.2.1.

### 3.4.1 Amendments for PSD2 Certificates

In case of EU Qualified Certificates for PSD2, the following requirements apply.

a) The CA SHALL document the procedure, which can be used for submission of certificate revocation requests by NCAs in its certificate policy or practice statement. The CA SHALL check the authenticity of certificate revocation requests submitted by NCAs.

Buypass documents the procedures in the CPS text in this document, see also 4.9.2.1 and 4.9.3.1.

Buypass accepts revocations requests from pre-registered and authorized representatives of the NCA. A revocation request from an NCA for a PSD2 Certificate will only be accepted if it comes from the NCA identified in the Certificate and the request is verified to come from an authorized representative for the NCA.

b) The CA shall provide an email address, or website in English or language understood by the NCAs served, for notifications from an NCA about changes of relevant PSD2 regulatory information of the PSP which can affect the validity of the certificate. The content and format of these notifications may be agreed between the NCA and CA. However, the CA shall investigate this notification regardless of its format.

Buypass offers a revocation management service which may also be used by NCAs for notifications of changes for the Subscriber of a PSD2 Certificate – see 4.9 a).

c) The CA shall recognize all of the following methods of authentication of the revocation request issued by the NCA:
   - a shared secret if it was provided by the CA to the NCA for revocation purposes,
   - a digital signature supported by a certificate issued to the NCA by a CA compliant with a QCP policy according to Regulation (EU) No 910/2014 [22]).

     NOTE: The digital signature can be used to provide an advanced electronic seal from the NCA or an advanced electronic signature from a signatory acting on behalf of the NCA.

Buypass accepts any revocation request signed by a pre-registered and authorized representative of the NCA or sealed by the NCA. Both qualified and advanced electronic signatures/seals will be accepted provided that they are supported by a qualified certificate.

d) If the CA is notified of an email address where it can contact the respective NCA then it should inform the NCA, using this email address, how the NCA can authenticate itself in revocation requests.

Buypass registers contact information for an NCA when obtained and informs the NCA about the revocation procedure.

# 4 Certificate life-cycle operational requirements

## 4.1 Certificate Application

A Certificate Application is a request from a Certificate Manager or Certificate Applicant to the RA/CA for the issuance of a Certificate.

### 4.1.1 Who Can Submit a Certificate Application

The application procedure consists of the following steps;

a) Subscriber Registration and Subscriber Agreement Signing: The Subscriber must register with Buypass all Subscriber information defined in 3.2.2 as well as any required proof of authorization for all registered Authorized Officers, Certificate Managers, Certificate Applicants and Subject Sponsors as described in 3.2.5. The Subscriber must also provide to Buypass a Subscriber Agreement signed by the Contract Signer.

b) Certificate Application Submission: A Certificate Manager or a Certificate Applicant identified and authorized as part of the step a) provides to Buypass a Certificate Application.

Step a) and b) may be performed in one operation. In that case, the Contract Signer is signing the Subscriber Registration, Subscriber Agreement and the Certificate Application at the same time.

a) Any Authorized Officer, Certificate Manager, Certificate Applicant, Subject Sponsor and Contract Signer MUST register with an RA as Authorized Subscriber Representatives either prior to, or at the time of, applying for a Certificate. 3.2 defines necessary requirements for identification and authorization.

All persons authorized by a Subscriber to exercise the Certificate Applicant, Certificate Manager, Authorized Officer and Contract Signer roles are registered as part of the Subscriber Registration step (step a above). Persons authorized to exercise the Subject Sponsor role may be identified at Certificate Application time.

b) Either the Authorized Officer, Certificate Manager, Certificate Applicant or the Subject Sponsor SHALL be authenticated as an Authorized Subscriber Representative towards an RA or RA representative as described in 3.2.5, either as part of the Certificate application process or as part of the Certificate issuance process.

For EU Qualified Certificates, the Authorized Officer must confirm the identity of the Subscriber by being authenticated according to 3.2.3.

The Subject Sponsor is authenticated face-to-face during personal delivery of the secret Distribution Key for a Soft Token or the token itself for a Hard Token in case of CA generated private keys (see 3.1.3 a).

For Subscriber generated private keys, the Certificate Applicant is authenticated during personal delivery of the Authorization Code.

A pre-authorized Certificate Applicant who is electronically authenticated (see 3.1.3 b) may act as the Subject Sponsor.

### 4.1.2 Enrollment Process and Responsibilities

a) The Subscriber SHALL accept the terms and conditions regarding the use of Buypass Class 3 Enterprise Certificates.

Terms and conditions regarding the use of the Certificates are made available to the Subscriber through a Subscriber Agreement. The Subscriber must accept the terms and conditions in order to complete the Certificate application.

b) The Subscriber SHALL provide to the RA:
- all Subscriber information as defined in 3.2
- a legally enforceable Subscriber Agreement signed by an authorized Contract Signer
- a Certificate Application signed by an authorized Certificate Manager or Certificate Applicant

No Certificate Application is approved by Buypass before all information above has been provided by the Subscriber.

c) If the Subscriber Agreement is in electronic form, it SHOULD be signed with an Advanced Electronic Signature or an Advanced Electronic Seal as specified by Regulation (EU) No 910/2014 [22].

Buypass accepts Subscriber Agreements in electronic forms signed with an Advanced Electronic Signature or Advanced Electronic Seal. However, this is not required.

d) The confidentiality and integrity of application data SHALL be protected, especially when exchanged between the Certificate Manager or Certificate Applicant and RA or between distributed RA/CA system components. The Certificate Applicant SHALL be able to establish the identity of the RA.

Buypass offers a TLS protected web-based RA service. The SSL Certificate identifies Buypass as the domain owner.

e) In the event that external RAs are used, the CA SHALL verifies that application data is exchanged with recognized RAs, whose identity is authenticated.

Buypass does not use external RAs or external registration service providers

## 4.2 Certificate application processing

The procedure of verifying the Certificate application performed by the RA or CA SHALL ensure:

- that the Certificate application is accurate and complete
- that the Authorized Officer, Certificate Managers and/or Certificate Applicant has been appropriately identified and authorized as a Subscriber Representative as described in 3.2.2.1
- that the submitted Subscriber information has been verified against the relevant national registers such as for example a QGR

For each Certificate Application processed, Buypass use established controls to ensure that:

- all mandatory Subscriber information (see 3.2) has been obtained from the Subscriber
- the Subscriber's Organization Name and Organization Number exist in a QGR
- authorization has been established for all registered Authorized Officers, Certificate Managers, Certificate Applicants, Subject Sponsors and Contract Signers as required by their respective role, see 3.1.2
- a registered Contract Signer has signed the Subscriber Agreement
- a registered Certificate Manager or Certificate Applicant has signed the Certificate Application

### 4.2.1 Performing Identification and Authentication Functions

### 4.2.2 Approval or Rejection of Certificate Applications

The Certificate Application SHALL be rejected if any of the verification steps in 4.2 fails. In this case the Certificate Applicant SHALL be notified without undue delay that the Certificate Application has been rejected.

The verification controls in 4.2 has been implemented using a combination of automated system controls and manual controls performed by authorized Buypass personnel.

Automated verification controls performed in-line during a Subscriber's use of Buypass' web-based RA service will result in immediate rejection of the Certificate Application. Otherwise, the Certificate Applicant is notified by phone or e-mail whenever the Certificate Application is rejected.

### 4.2.3 Time to Process Certificate Applications

## 4.3 Certificate issuance

### 4.3.1 CA Actions during Certificate Issuance

a) Certificate issuance will only take place after a Certificate application has been approved.

Generation of Certificates is initiated after the Certificate Application has been approved.

b) Two different schemes for Certificate issuance are supported dependent on whether:
- the Subject's key pair is generated by the CA
- the Subject's key pair is generated by the Subscriber

Buypass issues Enterprise certificates for both schemes.

c) The CA SHALL take measures against forgery of Certificates, and, in cases where the CA generates the Subjects' Private Key, guarantee confidentiality during the process of generating such data.

For CA generated Subject Keys, all Subject Private Key pairs are generated in an HSM within Buypass CA facilities (see 5.1). The process ensures that Private Keys are kept confidential at all times and that the only party that has access to the private keys after they have been generated is the Subscriber who has been issued the Certificate.

d) The procedure of issuing a Certificate, including the provision of any Subscriber generated Public Key, SHALL be securely linked to the associated initial Certificate application or rekey application.

Certificate Application data is integrity protected while in possession by Buypass to ensure that key pairs and Certificates are generated, linked and distributed to the correct Subscriber.

e) If the CA generates the Subject's Private Key, the procedure of issuing the Certificate SHALL be securely linked to the generation of the key pair by the CA.

For CA generated Subject Keys, Key generation and Certificate issuance is performed in one operation. Regarding secure Private Key distribution, see 6.1.2.

f) The Certificates that are issued SHALL follow the requirements defined in 7.

All Class 3 Enterprise Certificates issued follow the Certificate profile requirements defined in 7.

### 4.3.2 Notification of Certificate Issuance

a) The RA SHALL issue an out-of-band notification to the Subscriber once a Certificate has been issued.

Every time a new Class 3 Enterprise Certificate is issued for a Subscriber, Buypass sends a notification e-mail to the registered Certificate Applicant for that Subscriber.

b) Over the life time of the CA a distinguished name which has been used in a certificate by it shall never be re-assigned to another entity

The distinguished name in the Enterprise Certificate includes a country code and a unique, official registration number for the country where the Subscriber organization is registered. As long as the unique registration number is not reused for another entity in the country, the distinguished name will never be re-assigned another entity.

## 4.4 Certificate acceptance

### 4.4.1 Conduct constituting certificate acceptance

Unless the Subscriber gives notice to the contrary, the CA will assume that the Certificate, as it is made available, is accepted and deemed correct by the Subscriber.

The e-mail sent to the Certificate Applicant at time of issuance (see 4.2 g) describes how the Subscriber can verify Subscriber information in the Certificate.

The Subscriber is given a 2 weeks verification period to verify the Certificate and to notify Buypass in case the Subscriber information is incorrect.

If the Subscriber does not provide such a notification within this 2 weeks verification period, Buypass assumes that the Certificate, as it is made available, is accepted and deemed correct by the Subscriber.

However, the Subscriber is obliged to notify Buypass if any information in the Certificate is incorrect after this verification period.

### 4.4.2 Publication of the certificate by the CA

The CA SHALL ensure that the Certificates issued are made available as necessary to Subscribers and Relying parties.

When Buypass generates the Private Keys the following rules apply:

- For Soft Tokens, the Class 3 Enterprise Certificates are distributed to the Subscriber by attaching it as PKCS#12 files to an e-mail that is sent to the registered Certificate Applicant. The e-mail also includes a link to a web service presenting the Certificate for verification purpose.
- For Hard Tokens, the Class 3 Enterprise Certificates are distributed to the Subscriber in a smart card sent to the registered Subject Sponsor. The Certificates are also available for verification by the Certificate Applicant through a link in the notification e-mail sent.

When the Subscriber generates the Private Keys, the following rules apply:

- The Enterprise Certificate is sent to the Subscriber in an e-mail sent to the registered Certificate Applicant. The e-mail also includes a link to a web service presenting the Certificate for verification purpose.
- In addition, all Class 3 Enterprise Certificates that are issued are immediately made publicly available to Relying Parties through a public LDAP directory service.

### 4.4.3 Notification of certificate issuance by the CA to other entities

#### 4.4.3.1 Notification to NCA for PSD2 Certificates

If the CA is notified of an email address where it can inform the NCA identified in a newly issued certificate then the CA SHALL send to that email address information on the content of the certificate in plain text including the certificate serial number in hexadecimal, the subject distinguished name, the issuer distinguished name, the certificate validity period, as well as contact information and instructions for revocation requests and a copy of the a certificate file.

Buypass registers contact information for an NCA on request. When a PSD2 Certificate is issued, Buypass will send a notification email to the NCA identified in the Certificate using the pre-registered NCA contact information.

## 4.5 Key pair and certificate usage

### 4.5.1 Subscriber private key and certificate usage.

### 4.5.2 Relying party public key and certificate usage

## 4.6 Certificate renewal

The requirements in 4.1 SHALL apply also to a renewal application.

Renewal is only supported if the Subscriber generates the Private Key.

Buypass contacts the Subscriber by e-mail with information that an existing Certificate is about to expire two months before the Certificate's expiry date.

The Subscriber handles renewal using the same procedure as for the initial application, see 4.1.1. The "Subscriber Registration and Subscriber Agreement Signing" step may be omitted if the information registered during the original Subscriber registration is still valid.

If the renewal application is based on an existing Certificate about to expire, the lifetime of the new Certificate is calculated from the existing Certificate's expiry date.

If the renewal application is for a Certificate replacing an existing Certificate, the replacement Enterprise Certificate will be issued with the same expiry date as the existing Certificate. The existing Certificate will be revoked no later than 30 days after the new Certificate is issued.

### 4.6.1 Circumstance for certificate renewal

### 4.6.2 Who may request renewal

### 4.6.3 Processing certificate renewal requests

### 4.6.4 Notification of new certificate issuance to subscriber

### 4.6.5 Conduct constituting acceptance of a renewal certificate

### 4.6.6 Publication of the renewal certificate by the CA

### 4.6.7 Notification of certificate issuance by the CA to other entities

## 4.7 Certificate re-key

The requirements in 4.1 SHALL apply also to a rekey application, whether the Certificate application involves a routine rekey or a rekey after revocation.

Buypass contacts the Subscriber by e-mail or by phone with information that an existing Certificate is about to expire two months before the Certificate's expiry date.

The Subscriber handles rekey using the same procedure as for the initial application, see 4.1.1. The "Subscriber Registration and Subscriber Agreement Signing" step may be omitted if the information registered during the original Subscriber registration is still valid.

If the rekey application is based on an existing Certificate about to expire, the lifetime of the new Certificate is calculated from the existing Certificate's expiry date.

If the rekey application is for a Certificate replacing an existing Certificate, the replacement Enterprise Certificate will be issued with the same expiry date as the existing Certificate. A replacement Certificate can only be requested within the validity period of the existing Certificate. The existing Certificate will be revoked no later than 30 days after the new Certificate is issued.

### 4.7.1 Circumstance for certificate re-key

### 4.7.2 Who may request certification of a new public key

### 4.7.3 Processing certificate re-keying requests

### 4.7.4 Notification of new certificate issuance to subscriber

### 4.7.5 Conduct constituting acceptance of a re-keyed certificate

### 4.7.6 Publication of the re-keyed certificate by the CA

### 4.7.7 Notification of certificate issuance by the CA to other entities

## 4.8 Certificate modification

### 4.8.1 Circumstance for certificate modification

### 4.8.2 Who may request certificate modification

### 4.8.3 Processing certificate modification requests

### 4.8.4 Notification of new certificate issuance to subscriber

### 4.8.5 Conduct constituting acceptance of modified certificate

### 4.8.6 Publication of the modified certificate by the CA

### 4.8.7 Notification of certificate issuance by the CA to other entities

## 4.9 Certificate revocation and suspension

The CA SHALL ensure that Certificates are revoked in a timely manner based on authorized and validated Certificate revocation requests.

a) The CA SHALL offer a revocation management service. Revocations requests may be submitted 24 hours a day 7 days per week.

Buypass offers a 24x7 revocation service where Subscribers can submit revocation requests either by phone, e-mail or the Buypass Web.

Authorized Subscriber Representatives may in addition revoke Subscriber's Certificates through a web-based RA Service.

b) The maximum delay between receipt of a revocation request and the change to revocation status information being available to all Relying Parties SHALL be at most 24 hours.

The revocation request must be confirmed either by the Subscriber or by an Authorized Subscriber Representative before the revocation request processing can be completed.

Unless the revocation request processing concludes that the request is rejected, the Certificate will either be revoked or suspended at the latest 1 hour after confirmation of the request.

Relaying Parties using the Buypass OCSP service will be informed immediately after the Certificate has been suspended or revoked.

Relying Parties that depend on the Buypass CRL service will be informed about the suspension/revocation as soon as the next CRL is published. The next CRL will be published no later than 13 hours after confirmation of the revocation request.

c) Revocation status information SHALL be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the CA, the CA SHALL make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement.

Buypass offers revocation status information 24x7. Revocation status information is offered both as a CRL service and as an OCSP service.

The guaranteed service level for both these services in terms of availability are 99,8% and any loss of availability will not last more than 4 hours at a time.

Service information that is considered relevant for Subscribers and/or Relying Parties is published on Buypass Web.

d) The integrity and authenticity of the status information shall be protected.

Buypass offers a CRL service where the CRL is signed by the CA Private Key and an OCSP service where the OCSP response is signed either by the CA Private Key or a delegated OCSP Responder Private Key

e) Revocation status information SHALL include information on the status of Certificates at least until the Certificate expires.

For the CRL service, the revocation status information is available until the Certificate expires. For the OCSP service, the revocation status information is available until the CA is terminated.

f) The RA SHALL issue an out-of-band notification to the Subscriber once a Certificate has either been revoked or suspended.

The registered Certificate Applicant for a specific Class 3 Enterprise Certificate is notified by e-mail once the Certificate has either been revoked or suspended.

g) A revoked Certificate SHALL NOT be reinstated.

## 4.9.1 Circumstances for Revocation

#### 4.9.1.1 Reasons for Revoking a Subscriber Certificate

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

- the Subscriber requests revocation of its Certificate
- the Subscriber notifies the CA that the original Certificate Application was not authorized and does not retroactively grant authorization
- the CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate has been compromised or no longer complies with the requirements of 6.1.1.3, 6.1.5 and 6.1.6
- The CA obtains evidence that the Certificate was misused
- the CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement
- the CA is made aware of a material change in the information contained in the Certificate
- the CA is made aware that the Certificate was not issued in accordance with the applicable Certificate Policy [20] or the Certification Practice Statement [21]
- the CA determines that any of the information appearing in the Certificate is inaccurate or misleading
- the CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate
- the CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate
- the technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time)
- the Subscriber does not pay the service fees to Buypass (see 9.1.1)

- the Subscriber ceases to exist
- the NCA requests revocation for a PSD2 certificate where the Subscriber (PSP) who has lost its authorization to act as a PSP or any PSP role in the certificate has been removed

#### 4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

- the Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Subordinate CA Certificate has been compromised or no longer complies with the requirements of 6.1.1.1, 6.1.5 and 6.1.6
- the Issuing CA obtains evidence that the Subordinate CA Certificate was misused
- the Issuing CA is made aware that the Subordinate CA Certificate was not issued in accordance with or that Subordinate CA has not complied with the Certificate Policy [20] or Certification Practice Statement [21]
- the Issuing CA determines that any of the information appearing in the Subordinate CA Certificate is inaccurate or misleading
- the Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Subordinate CA Certificate
- the technical content or format of the Subordinate CA Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time)

### 4.9.2 Who Can Request Revocation

a) Only Authorized Subscriber Representatives MAY request Certificate revocation on behalf of the Subscriber.

Certificate revocation may be requested either by the Subscriber or one of the Authorized Subscriber Representatives already registered with Buypass for that particular Subscriber.

Buypass accepts revocation requests from unregistered Subscriber Representatives only if

a) the revocation request is confirmed either by the Subscriber or an existing Authorized Subscriber Representative, or

b) Buypass, through further investigation, has reason to believe that a valid revocation reason exists (see 4.9.1.1)

b) The CA may revoke a Certificate or a Subordinate CA Certificate if the CA has reason to believe that a valid revocation reason exists.

Buypass is entitled to, and will request revocation of a Subscriber's Certificate or a Subordinate CA Certificate, at any time for any of the reasons set forth in 4.9.1.

c) Revocation requests received from a non-authorized requestor SHALL be investigated by the CA and the Subscriber SHALL be consulted if necessary.

If a revocation request is received and if Buypass is not able to establish the requestor as an Authorized Subscriber Representative, Buypass will contact an Authorized Subscriber Representative in order to confirm the revocation request. If this is not possible Buypass will make an effort to check whether there is a valid revocation reason.

#### 4.9.2.1 Amendments for PSD2 Certificates

The CA SHALL allow the NCA, as the owner of the PSD2 specific information, to request certificate revocation following the procedure defined in the CA's certificate policy or certificate practice statement. The procedure

shall allow the NCA to specify a reason, which can be descriptive rather than in a standard form, for the revocation.

Buypass accepts revocation requests from pre-registered and authorized representatives of the NCA.

Buypass offers a revocation management service which may also be used by NCAs for notifications of changes for the Subscriber of a PSD2 Certificate – see 4.9 a). This service allows the NCA to specify a reason in a descriptive form.

### 4.9.3 Procedure for Revocation Request

a) Authorized Subscriber Representatives MAY submit revocation requests to an RA either in person, by writing, by telephone or through electronic communication. The possibilities that are offered SHALL be made available to the Subscriber.

Buypass offers a 24x7 revocation service where Subscribers can submit revocation requests by phone, e-mail or the Buypass Web. Contact points for revocation are communicated to the Subscriber through the Subscriber Agreement and are available on Buypass Web.

b) Revocation requests SHALL be authenticated and checked to be from an authorized source. The CA SHALL document detailed procedures for how RAs shall authenticate the originator of a revocation request.

Whenever a revocation request is received by Buypass, Buypass RA personnel (i.e. a Revocation Officer) will operate according to documented routines that describe the different controls that need to be executed before the request is authorized and revocation is performed.

#### 4.9.3.1 Amendments for PSD2 Certificates

a) The CA shall process such requests, and shall validate their authenticity. If it is not clearly indicated or implied why the revocation is requested or the reason is not in the area of responsibility of the NCA then the TSP may decide to not take action. Based on an authentic request from an NCA, the CA shall revoke the certificate in a timely manner if any of the following conditions holds (in addition to any general requirements of ETSI EN 319 411-2 [5]):
   - the authorization of the PSP has been revoked;
   - any PSP role included in the certificate has been revoked

Buypass accepts any revocation request signed by a pre-registered and authorized representatives of the NCA or sealed by the NCA – see 3.4.1.

Buypass accepts that the Subscriber has lost its authorization to act as a PSP or that any PSP role in the certificate has been removed as valid revocation reasons – see 4.9.1.1.

b) The CA shall provide an email address, or website in English or language understood by the NCAs served, where an NCA can submit authenticated revocation requests and other notifications relating to revocation.

Buypass offers a revocation management service which may also be used by NCAs for notifications of changes for the Subscriber of a PSD2 Certificate – see 4.9 a).

See also 3.4.1 c) for how to verify the authenticity of revocation requests from an NCA.

c) If the NCA as the owner of the PSD2 specific information notifies the CA, that information has changed which can affect the validity of the certificate, but without a properly authenticated request with an acceptable reason for why the certificate should be revoked, the CA shall investigate this notification regardless of its content and format, and shall revoke the affected certificate(s) if necessary. This notification need not be processed within 24 hours.

The NCA may notify Buypass about changes in information related to a specific PSD2 certificate by several means.

Buypass will try to verify that the revocation request is authentic, but if this is not possible, Buypass will make an effort to investigate whether there is a valid revocation reason.

d) If the CA is notified of an email address where it can inform the NCA identified in a revoked certificate then the CA SHALL send to that email address information about the certificate revocation.

Buypass maintains contact information for NCAs. When a PSD2 Certificate is revoked, Buypass will send a notification email to the NCA identified in the Certificate using the pre-registered NCA contact information.

### 4.9.4 Revocation Request Grace Period

a) For revocation reasons other than key compromise, the Subscriber SHALL request revocation as soon as possible after a valid revocation reason is known.

b) For revocation reason key compromise, see 4.9.12.

### 4.9.5 Time within which CA Must Process the Revocation Request

### 4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties SHALL check either the latest CRL or use the online Revocation status service (4.9.9) in order to establish whether any of the Certificates in the certification path have been revoked.

### 4.9.7 CRL Issuance Frequency

a) The CA SHALL provide a CRL service.

Buypass provides a CRL service where CRLs may be accessed using the HTTP protocol.

The URL is included in the CRL Distribution Point extension of all Class 3 Enterprise Certificates that are issued.

b) The CRL service for Subscriber Certificates SHALL at least issue CRLs every 24 hours and each CRL SHALL have a maximum expiration time of 48 hours.

Buypass issues and publishes a new CRL for Subscriber Certificates every 12 hours. A new CRL may be published at other times, e.g. after a Certificate is revoked or suspended. The expiration time for each CRL is 25 hours.

Monitoring is in place to ensure early detection and response if the process of CRL generation and CRL publishing fails.

c) The CA SHALL perform capacity planning at least annually to operate and maintain its CRL service to commercially reasonable response times.

Capacity planning for all services covered by this document is performed regularly and at least once a year.

### 4.9.8 Maximum Latency for CRLs

### 4.9.9 On-line Revocation/Status Checking Availability

a) The CA SHALL provide an online revocation status services.

Buypass provides an online OCSP service. The service URL is included in the AIA extension of all Certificates.

b) The revocation status information SHALL be made available beyond the validity period of the Certificate.

The OCSP service is available for all Certificates beyond the validity period of the Certificate. The OCSP status service will be available until the CA issuing the Certificate is terminated – see 5.8.

c) The CA SHALL perform capacity planning at least annually to operate and maintain its OCSP service to commercially reasonable response times.

Capacity planning for all services covered by this document is performed regularly and at least once a year.

### 4.9.10 On-line Revocation Checking Requirements

Relying parties SHALL check either the latest CRL (see 4.9.7) or use the online revocation status service (see 4.9.9) in order to establish whether any of the Certificates in the certification path have been revoked or not.

### 4.9.11 Other Forms of Revocation Advertisements Available

### 4.9.12 Special Requirements Related to Key Compromise

In case of suspected or known compromise of a Subscriber's Private Key, a revocation request SHALL be promptly submitted.

### 4.9.13 Circumstances for Suspension

a) If an RA is not able to process a Certificate revocation request in due time (see 4.9.2 c), the Certificate SHALL be suspended until the revocation request has been properly processed.

b) If a Certificate has been suspended as a result of a), the Certificate SHALL either be revoked or unsuspended once the revocation request has been properly processed.

### 4.9.14 Who Can Request Suspension

Certificate suspension can only be requested by an RA.

### 4.9.15 Procedure for Suspension Request

The RA SHALL submit a suspension request to the CA whenever the criteria for suspension is fulfilled (see 4.9.13).

If there is reason to believe that a valid revocation reason exists, the RA may suspend the Certificate until the revocation reason has been confirmed or rejected.

### 4.9.16 Limits on Suspension Period

A Certificate that has been suspended SHALL be revoked or unsuspended at the latest 30 days after the Certificate was suspended.

For a suspended Certificate, the original Certificate revocation request is processed in due time to ensure that the Certificate is either revoked or unsuspended at the latest 30 days after the Certificate was suspended.

## 4.10 Certificate status services

### 4.10.1 Operational Characteristics

### 4.10.2 Service Availability

### 4.10.3 Optional Features

## 4.11 End of subscription

## 4.12 Key escrow and recovery

### 4.12.1 Key escrow and recovery policy and practices

### 4.12.2 Session key encapsulation and recovery policy and practices

# 5 Management, operational, and physical controls

a) The CA SHALL implement Computer Security Controls according to best practice according to ISO/IEC 27002:2013 [11] and in compliance with Buypass Information Security Policy [3].

Buypass' Information Security Management System (ISMS) has been certified against ISO/IEC 27001:2013 where Buypass' Information Security Policy is the governing document.

Buypass' ISMS is reasonably designed to:

a) Comply with ISO/IEC 27002:2013 as constrained by Buypass' statement of applicability (SOA);

b) Comply with the security requirements defined by ETSI EN 319 401 [14], ETSI EN 319 411-1 [16] and ETSI EN 319 411-2 [17];

c) Protect the confidentiality, integrity, and availability of: (i) all Certificate Requests and data related thereto (whether obtained from Applicant or otherwise) in CA's possession or control or to which CA has access, and (ii) the keys, software, processes, and procedures by which the CA verifies Data, issues Certificates, maintains a repository, and revokes Certificates;

d) Protect against any identified threats to the confidentiality, integrity, and availability of the Data and Processes;

e) Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Data or Processes;

f) Protect against accidental loss or destruction of, or damage to, any Data or Processes; and

g) Comply with all other security requirements applicable to the CA by Norwegian law.

b) The CA's security program MUST include an annual Risk Assessment that:
   1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
   2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
   3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Buypass performs an annual Risk Assessment based on the ETSI processes:

- Registration Service
- Certificate generation Service
- Dissemination Service
- Revocation Management Service
- Revocation Status Service

Based on such Risk Assessment, Buypass develops, implements, and maintains security procedures, measures, and products to reasonably manage and control the risks identified during the Risk Assessment. This includes administrative, organizational, technical, and physical security measures and controls.

## 5.1 Physical security Controls

### 5.1.1 Site location and construction

Physical and environmental security controls SHALL be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The CA's physical and environmental security policy for systems associated with Certificate generation and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc.

All Buypass' operations facilities are specifically designed for computer operations and have been customized to meet the security requirements that apply to Buypass as a CA. Relevant prevention and detection mechanisms are in place to address environmental incidents, hereunder power loss, loss of communication, water exposure, fire and temperature changes.

### 5.1.2 Physical access

a) Physical access to facilities associated with Certificate generation and revocation management services SHALL be limited to properly authorized individuals.

Access to Buypass' CA/RA facilities are restricted to authorized Buypass personnel only. Non-authorized personnel, including visitors, are only allowed to access the facilities under escort and continuous surveillance by authorized personnel.

Dual control has been implemented for physical access to the CA operations facilities. Access requires physical presence of two authorized persons, each with their own personal two factor authentication token.

b) Any persons entering this physically secure area SHALL be followed by an authorized person and NOT left alone any time.

Current routines ensure that no authorized person will stay in the CA operations facilities alone for any significant period of time. Non-authorized persons are not at any circumstances permitted to stay alone within the CA operations facilities.

c) Physical protection SHALL be achieved through the creation of clearly defined security perimeters. Any parts of the premises shared with other organizations shall be outside this perimeter.

Access to Buypass' CA/RA facilities is protected with several tiers of clearly defined security perimeters. The inner tiers are dedicated to Buypass' operations alone and are only accessible to authorized Buypass personnel.

d) Controls SHALL be implemented to protect against equipment, information, media and software relating to the CA services being taken off-site without authorization.

Buypass maintains procedures that cover secure and trusted asset handling, including transport of security sensitive assets off-site. Physical controls such as restricted access with dual access control and regular inventory control are designed to prevent and detect unauthorized movement assets.

e) Other functions relating to CA operations may be supported within the same secured area provided that the access is limited to authorized personnel.

Other functions related to Buypass role as e.g. an Identity Provider, Payment Service Provider are supported in the same secured area with the same access restrictions as for the CA operations.

f) Root CA Private Keys shall be held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA certificates.

Buypass Root CA Private Keys are held and used in standalone and air gapped equipment. All operations using the Root CA Private Keys are authorized by three Security Officers.

### 5.1.3 Power and air conditioning

### 5.1.4 Water exposures

### 5.1.5 Fire prevention and protection

### 5.1.6 Media storage

### 5.1.7 Waste disposal

### 5.1.8 Off-site backup

## 5.2 Procedural controls

### 5.2.1 Trusted Roles

a) All personnel engaged in CA related tasks are considered trusted personnel. The following trusted roles are defined:
- Security Manager, is overall responsible for administrating the implementation of security policies and practices and formally appoints personnel to the other trusted roles
- Security Officer, is responsible for the implementation of the security practices
- System Auditor, controls that routines are complied with and reads archives and audit logs
- System Administrator, is responsible for the installation, configuration and maintenance of security software and hardware
- System Operator, is responsible for the operation of systems on a day-to-day basis and authorized to perform system backup and recovery
- Registration Officer, responsible for approving end entity Certificate generation and revocation
- Revocation Officer, responsible for approving end entity Certificate revocation

Buypass continuously maintains an overview of which persons that either possesses or has possessed the defined roles at any point in time.

b) Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the CA assets.

Controls are in place to ensure segregation of duties in that no person can assume several conflicting roles.

c) The CA SHALL employ a sufficient number of personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.

Buypass continuously ensures a staffing of qualified personnel sufficient to maintain the required segregation of duties as well as the target service level. An overview of experience and qualifications for all personnel involved in CA/RA operations is maintained. Risk and vulnerability assessments that are performed regularly include an evaluation of personnel qualifications.

### 5.2.2 Number of Individuals Required per Task

a) Certificate issuance by the root CA shall be under at least dual control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own

All use of Root CA Private Keys are authorized by three Security Officers.

b) All maintenance operations involving CA private keys SHALL be under at least dual control by authorized, trusted personnel.

Generation of CA Private Keys are authorized by three Security Officers.

Installation and activation of cryptographic modules containing CA Private Keys are performed by two persons assuming a System Operator role.

Destruction of CA Private Keys are witnessed by three persons assuming a Security Officer role.

c) All other CA system operations MAY be performed by a single person.

Buypass may decide to implement dual control for other CA/RA operations if considered needed on the basis of regular risk and vulnerability assessments.

### 5.2.3 Identification and Authentication for Trusted Roles

No stipulations.

All personnel assuming one of the trusted roles defined in 5.2.1 are Buypass employees. Appropriate identification and face-to-face authentication is handled as part of the employment procedure.

In order to perform their duties as trusted personnel, authentication is required for physical access to CA/RA facilities (see 5.1) as well as for logical access to CA/RA systems.

All trusted personnel able to approve certificate requests and/or issue certificates must authenticate themselves using a two-factor smart card authentication.

### 5.2.4 Roles Requiring Separation of Duties

## 5.3 Personnel controls

The CA SHALL ensure that personnel and employment/contractor practices maintain and support the trustworthiness of the CA's operations.

### 5.3.1 Qualifications, Experience, and Clearance Requirements

a) The Security Manager is responsible for ensuring that CA personnel have undergone necessary background checks and training before they are appointed trusted roles.

Buypass' Human Resources Department has the overall responsibility that persons assuming trusted roles have passed defined background checks and that they have gone through necessary education/training.

A written role instruction exists for each trusted role that includes a requirement for maintaining a personal competency plan. Implementation of this plan in terms of ensuring appropriate training at the time a person first assumes a particular role as well as subsequent refreshment training when needed is the responsibility of each person's superior manager within the Buypass organization.

b) CA personnel SHALL provide proof of their identity, background, qualifications and experience, as well as any other information required by the CA.

Thorough reference checks, including confirmation of previous employments and relevant education, are used prior to authorizing a person to assume one of the trusted roles as defined in 5.2.1.

c) CA personnel SHALL be given necessary CA operations and security training. Training programs SHALL be targeted individually, dependent on existing qualifications and experience of the trainee.

General security training is provided at the time of employment and regularly thereafter. Specific training for persons assuming trusted roles is managed through individual competency plans, see 5.3.1 a).

d) CA personnel SHALL be free from conflicting interests that might prejudice the impartiality of the CA operations.

Potential conflict of interests is evaluated for all persons that are to assume a trusted role.

e) The parts of the CA concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies; in particular its senior executive, senior staff and staff in trusted roles, shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

The parts of the Buypass CA associated with certificate generation and revocation management are structured independently of the Buypass organization structure to ensure that important decisions regarding the CA operation are taken with impartiality of other parts of Buypass and other organizations.

f) The parts of the CA concerned with certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.

The structure of the parts of the Buypass CA associated with certification generation and revocation management are documented and communicated to all persons involved in the operations.

### 5.3.2 Background Check Procedures

a) The CA's management is responsible for ensuring that necessary background checks are completed for all trusted personnel.

Se 5.3.1 a)

b) The CA SHALL NOT appoint to trusted roles any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position.

Any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position will not be authorized by Buypass to assume a trusted role as defined in 5.2.1.

### 5.3.3 Training Requirements and Procedures

### 5.3.4 Retraining Frequency and Requirements

For all CA personnel in trusted roles the CA SHALL evaluate the need for retraining at least once a year.

The need to refresh knowledge for personnel assuming trusted roles is evaluated at least once a year by the person responsible for the Buypass CA services.

### 5.3.5 Job Rotation Frequency and Sequence

No stipulations.

Job rotation may be introduced if deemed necessary based on regular threat and vulnerability assessments.

### 5.3.6 Sanctions for Unauthorized Actions

a) Appropriate disciplinary sanctions SHALL be applied to personnel violating the Certificate Policy [20] or underlying operative procedures.

Buypass' Chief Security Officer is responsible for making trusted personnel aware of consequences and disciplinary actions as a result of security violations as seen in the context of the Certification Practice Statement [21] and supporting operational routines.

b) Measures SHALL be established whereby all authorizations for trusted persons can be immediately revoked, so that a non-trusted person can be neutralized before doing harm.

Routines are in place that promptly enables Buypass to revoke a person's access to Buypass facilities and systems if it is revealed that a trusted person has acted in an unauthorized manner and/or in a way that that Buypass no longer has necessary trust in this person. A decision to revoke a person's access is taken by the Buypass' Operations Manager together with Buypass' Chief Security Officer.

### 5.3.7 Independent Contractor Controls

Independent contractors or consultants MAY possess trusted positions subject to the contractors or consultants being trusted by the CA to the same extent as if they were employees. Otherwise, independent contractors and consultants shall have access to secure facilities only to the extent they are escorted and directly supervised by Trusted Personnel.

Persons assuming trusted roles as defined in 5.2.1 are employees of Buypass.

### 5.3.8 Documentation Supplied to Personnel

The CA's management SHALL provide direction on information security through a suitable high level steering forum that is responsible for defining the CA's information security policy and ensuring publication and communication of the policy to all employees who are impacted by the policy.

Buypass ensures that all employees are familiar with the Buypass' information security policy and that employees involved in the provisioning of CA/RA services as specified in 9.6 are familiar with the Certificate Policy [20] and the Certification Practice Statement [21]. Both documents are available electronically.

## 5.4 Audit logging procedures

### 5.4.1 Types of Events Recorded

The CA SHALL ensure that records of all relevant events and related information regarding the services defined in 9.6.1 are retained for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.

a) The CA SHALL record in detail every action taken to process an Certificate Application and to issue a Certificate, including all information generated or received in connection with a Certificate Application, and every action taken to process the Application, including time, date, and personnel involved in the action. These records SHALL be available as auditable proof of the CA's practices. The foregoing also applies to all Registration Authorities (RAs) and subcontractors as well.

See 5.4.1 g)

b) All events related to registration including requests for certificate re-key or renewal shall be logged

c) All registration information including the following shall be recorded:

i. type of document(s) presented by the applicant to support registration;
ii. record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;
iii. storage location of copies of applications and identification documents, including the signed Subscriber Agreement
iv. identity of entity accepting the application;
v. method used to validate identification documents, if any; and
vi. name of receiving CA and/or submitting Registration Authority, if applicable.

See 5.4.1 g)

d) The CA shall record all the information necessary to verify the subject's identity and if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.

See 5.4.1 g)

e) The CA SHALL record the signed agreement with the Subscriber

Buypass records the Subscriber Agreement signed by the authorized Contract Signer – see 4.1.2

f) The CA shall maintain the privacy of subject information.

See 9.4

g) The record requirements in a) include, but are not limited to, an obligation to record the following events:
1. CA key lifecycle management events, including:
   - key generation, backup, storage, recovery, archival, and destruction
   - cryptographic device lifecycle management events
2. Certificate lifecycle management events, including:
   - Certificate Applications, rekey applications, renewal applications and revocation requests
   - all verification activities required
   - date, time, phone number used, persons spoken to, and end results of verification telephone calls
   - acceptance and rejection of Certificate Applications
   - issuance of Certificates
   - suspension and revocation of Certificates
   - generation of Certificate Revocation Lists (CRLs) and OCSP entries
3. security events, including:
   - changes relating to the security policy
   - system start-up and shutdown
   - successful and unsuccessful PKI system access attempts
   - PKI and security system actions performed
   - security profile changes
   - system crashes, hardware failures, and other anomalies
   - firewall and router activities
   - entries to and exits from the CA facility

For all Buypass CA/RA services and related processes, Buypass ensures that appropriate audit logs are produced that can provide auditable proof of events that is considered to have potential value as evidence in possible future disputes and/or legal proceedings. Audit logging covers, but is not limited to, the events that are listed above. Audit logs retained may be a combination of electronic logs and paper based logs.

Each audit log entry contains an event description, date/time of event, and a reference to which person or system that triggered the event.

h) For each log event, the following elements SHALL be recorded:
- date and time of event
- type of event
- identity of the entity responsible for the action
- success or failure for the event
- description of event

See 5.4.1 g)

### 5.4.2 Frequency for Processing and Archiving Audit Logs

a) Audit logs that indicate possible system compromise and/or unauthorized access to system resources SHALL be processed and reviewed at least once a day to identify evidence of malicious activity.

Security relevant audit logs that are system generated and that may indicate system compromise and/or unauthorized access to system resources are automatically processed every day against a predefined set of rules. Audit logs concerning physical access to Buypass operations facilities are regularly processed to ensure that all only authorized persons have had access. Other logs are processed as needed.

Buypass regularly evaluates which logs to include in every audit log processing, the frequency for such processing and which rule set to apply. Detected security incidents and anomalies are reported and managed according to Buypass' routine for security incidents.

b) Other audit logs SHALL be processed as needed.

See 5.4.2 a)

c) Controls SHALL be in place to ensure that events are recorded continuously and as intended.

Processes responsible for audit logging are continuously monitored and an alarm is triggered if the audit logging is either turned off or the audit logging configuration is changed.

### 5.4.3 Retention Period for Audit Logs

See 5.5.2.

### 5.4.4 Protection of Audit Log

a) Audit logs SHALL be stored in physically secured premises with access control.

Audit logs are stored in Buypass controlled restricted-access facilities (see 5.1) where only a few persons in trusted roles have access. This applies to current logs, archived logs and their backup copies. Integrity protection of all audit logs is maintained during backup and storage.

b) The confidentiality and integrity of current and archived audit records SHALL be maintained within the period of time that they are required to be held.

Only a few persons in trusted roles have access to the audit logs.

### 5.4.5 Audit Log Backup Procedures

There SHALL be offsite backup of all audit logs.

Buypass performs regular off-site backup of all security relevant audit logs. See also 5.4.4 a)

### 5.4.6 Audit Log Accumulation System (internal vs. external)

No stipulations.

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by Buypass personnel.

### 5.4.7 Notification to Event-Causing Subject

No stipulations.

All Buypass personnel has been informed that security auditing is being performed. Security incidents are handled according to predefined security procedures.

### 5.4.8 Vulnerability Assessments

No stipulations.

Audit logging is an integral part of a regular Risk and vulnerability analysis performed by Buypass. A periodic review is also performed on the predefined sets of rules that are used for audit log processing.

## 5.5 Records archival

### 5.5.1 Types of Records Archived

### 5.5.2 Retention Period for Archive

Audit records related to service events (see 9.6.1 for services definition) and that can be of relevance as evidence in legal proceedings concerning a particular Certificate SHALL be retained for at least 10 years after the Certificate either has expired or has been revoked.

Relevant audit records are retained and archived for at least 10 years after the Certificates that they concern have either expired or been revoked. This includes copies of all Certificates issued.

### 5.5.3 Protection of Archive

Audit records concerning Certificates SHALL be completely and confidentially archived in accordance with disclosed business practices.

Audit records are archived regularly. The archive is kept in secure on-site storage only accessible to trusted Buypass personnel. An off-site backup of the archived audit records exists.

### 5.5.4 Archive Backup Procedures

### 5.5.5 Requirements for Time-stamping of Records

### 5.5.6 Archive Collection System (internal or external)

### 5.5.7 Procedures to Obtain and Verify Archive Information

a) Audit records concerning Certificates SHALL be made available to independent auditors upon request and when required for the purposes of providing evidence for the purpose of legal proceedings.

In case of doubt whether errors has been made during the execution of the CA/RA services that Buypass is responsible for (see 9.6.1), then Buypass will, upon request, make archived audit records available to independent auditors as needed for the purpose of being used as evidence during legal proceedings.

b) The information that Subscribers contribute to the CA SHALL be completely protected from disclosure without the Subscriber's agreement, a court order or other legal authorization.

Buypass will neither publish nor disclose information registered about Subscribers and/or Subscriber Representatives without the Subscriber's explicit consent, a court order or other legal authorization. This includes information that is considered confidential according to 9.3.

c) The Subscriber SHALL have access to registration information and other information relating to the Subscriber.

Upon written request from the Subscriber, Buypass will disclose information that is registered about the Subscriber and/or Subscriber Representatives.

## 5.6 Key changeover

a) The CA SHALL perform a CA key changeover when the CA Certificate approaches the end of its lifetime or as required by the algorithms and key lengths used by the CA Certificate (see 6.1.5).

Buypass ensures that the CA key changeover will take place in due time before the CA certificate expires.

Buypass also continuously monitors the recommendations regarding cryptographic algorithms and key lengths to ensure that the CA issuing Certificates operates properly and according to best practices.

b) Key changeover SHOULD be performed with a suitable interval between certificate expiry date and the last certificate signed to allow all parties that have relationships with the CA (Subjects, Subscribers, Relying Parties, CAs higher in the CA hierarchy, etc.) to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply to a CA which will cease its operations before its own certificate-signing certificate expiration date.

Buypass will notify all Subscribers, Partners and Relying Parties in due time before the key changeover takes place.

c) The new CA Certificate with the new CA Public Key will be made available to Relying Parties following the same security requirements as defined in 6.1.4.

See 6.1.4

## 5.7 Compromise and disaster recovery

### 5.7.1 Incident and Compromise Handling Procedures

The CA SHALL ensure in the event of a disaster, including compromise or suspected compromise of the CA's private signing key, that operations are restored as soon as possible.

The CA SHALL define and maintain a business continuity plan (or disaster recovery plan) and this shall address the compromise, loss or suspected compromise of a CA's private key as a disaster and the planned processes shall be in place.

Buypass maintains both a business continuity plan and a separate disaster recovery plan. Both plans are supported by a set of routines and procedures that specifically covers the CA/RA services. The disaster recovery plan covers preoperational activities as well as activities taken after a disaster, hereunder off-site recovery of all services if required. Two redundant operations locations are available as well as an off-site disaster recovery location at one of the Buypass premises.

### 5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

a) Back-up copies of essential information and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure. Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.

Backups are performed daily at both sites and several versions are stored. All critical CA systems runs at two physically separate sites for continuous operations and direct fail-over. Full CA operations will be resumed within 24 hours. Physical and logical security controls are in place to prevent un-authorized access to backup systems

On-site data backup is performed several times a day and relevant data for recovery is replicated several times a day to an off-site location situated according to best practice on the area of continuity management. CA operations will be resumed within maximum 24 hours. Physical security controls are in place to prevent non-authorized access to both on-site and off-site backups.

b) Backup and restore functions SHALL be performed by people assuming the relevant trusted roles specified in 5.2.1.

Backup and restore routines are performed by Buypass personnel having a trusted System Operator role.

c) If risk analysis identifies information requiring dual control for management, for example keys, then dual control should be applied to recovery.

Dual control will be applied for recovery of keys according to protection level defined for the keys

### 5.7.3 Recovery Procedures After Key Compromise

a) In the case of a CA Key compromise the CA SHALL as a minimum provide the following undertakings:
- inform the following of the compromise: all Subscribers and other entities with which the CA has agreements or other form of established relations. In addition, this information SHALL be made available to other Relying Parties
- indicate that Certificates and revocation status information issued using this CA key may no longer be valid
- revoke any CA certificate that has been issued for the compromised CA

The business continuity plan covers CA Key compromise. The above undertakings are part of the supporting routines and procedures.

b) Should any of the algorithms, or associated parameters, used by the CA or its Subscribers become insufficient for its remaining intended usage then the CA SHALL:
- inform all Subscribers and Relying Parties with whom the CA has agreement or other formal established relations. In addition, this information SHALL be made available to other Relying Parties
- schedule a revocation of any affected Certificates

The business continuity plan covers algorithm compromise. The above undertakings are part of the supporting routines and procedures.

### 5.7.4 Business Continuity Capabilities after a Disaster

Following a disaster the CA SHALL, where practical, take steps to avoid repetition of a disaster.

Following a disaster, the disaster recovery plan specifies that a debrief will be conducted. Existing routines and security measures will be evaluated and appropriate actions will be taken to avoid repetition.

## 5.8 CA or RA termination

The CA SHALL ensure that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation of the CA's services, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

a) The CA SHALL have an up-to-date termination plan.

Buypass has a Buypass CA termination plan.

b) Before the CA terminates its services the following procedures SHALL be executed as a minimum:
- the CA SHALL inform the following of the termination: all Subscribers, Relying Parties and other entities with which the CA has agreements or other form of established relations. In addition, this information shall be made available to other Relying Parties
- the CA SHALL terminate all authorization of subcontractors to act on behalf of the CA in the performance of any functions related to the process of issuing Certificates
- the CA SHALL perform necessary undertakings to transfer obligations for maintaining registration information, revocation status information and event log archives for their respective period of time as indicated to the Subscriber and Relying Party
- CA private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved;
- where possible the CA SHOULD make arrangements to transfer provision of trust services for its existing customers to another provider
- the revocation of unexpired unrevoked Subscriber Certificates, if required

The Buypass CA termination plan includes all requirements above.

c) The CA SHALL have an arrangement to cover the costs to fulfil these minimum requirements in case the CA becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

Buypass has the necessary arrangements and agreements with 3rd party in place for continued operations and fulfilment of obligations in case of bankruptcy.

d) The CA SHALL state in its practices the provisions made for termination of service. This shall include:
- notification of affected entities
- transferring the CA obligations to other parties
- the handling of the revocation status for unexpired certificates that have been issued

The provisions are stated in the Buypass CA termination plan.

e) The CA SHALL maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period..

Buypass has the necessary arrangements and agreements with 3rd party in place for continued operations.

# 6 Technical security controls

## 6.1 Key pair generation and installation

### 6.1.1 Key Pair Generation

#### 6.1.1.1 CA Key Pair Generation

a) CA key pair generation and the subsequent certification of the public key, SHALL be undertaken in a physically secured environment (see 5.1) by personnel in trusted roles under, at least, dual control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

CA Key ceremonies are conducted in the CA operations facilities, using standalone and air gapped equipment. All operations are authorized by three Security Officers.

Ceremonies involving generation of Root CA Private Keys are under supervision of an independent auditor.

b) The CA SHALL have a documented procedure for conducting CA key pair generation for all CAs, whether root CAs or subordinate CAs, including CAs that issue certificates to end users. This procedure shall indicate, at least, the following:
- Roles participating in the ceremony (internal and external from the organization);
- Functions to be performed by every role and in which phases;
- Responsibilities during and after the ceremony; and
- Requirements of evidence to be collected of the ceremony

Buypass has documented procedures for the key ceremonies covering all elements described above.

c) The CA SHALL produce a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. This report shall be signed:
- For root CA: by the trusted role responsible for the security of the CA's key management ceremony (e.g. security officer) and a trustworthy person independent of the CA management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.
- For subordinate CAs: by the trusted role responsible for the security of the CA's key management ceremony (e.g. security officer) as witness that the report correctly records the key management ceremony as carried out.

Buypass produces a ceremony report signed by participants of the ceremony

d) The CA private signing key SHALL be generated within a cryptographic device which either:
- meets the requirements identified in ISO/IEC 19790 [9] or FIPS PUB 140-2 [5] level 3; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC15408 [12], or national or internationally recognized evaluation criteria for IT security. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures

The Buypass Class 3 CA Private Keys are or will be generated in an HSM compliant to FIPS 140-2 level 3.

e) A suitable time before expiration of its CA signing key (for example as indicated by expiration of CA Certificate), the CA SHALL generate a new Certificate-signing key pair and SHALL apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key shall also be generated and distributed in accordance with this policy.

See 5.6.

#### 6.1.1.2 RA Key Pair Generation

#### 6.1.1.3 Subscriber Key Pair Generation

**Subject key generation performed by the CA**

a) The CA SHALL ensure that any Subject keys are generated securely and the secrecy of the subject's Private Key is assured.

The Subject Private Keys are generated in an HSM compliant to FIPS 140-2 level 3.

b) CA generated subject keys SHALL be generated and stored securely before delivery to the subject.

For Soft Tokens, the Subject Private Key is stored encrypted in a PKCS#12 file, protected with a secret Distribution Key.

The Private Key is embedded within the PKCS#12 file within the HSM and the Private Key is never available in clear text outside the HSM.

c) The CA SHALL secure the issuance of a secure cryptographic device to the subject. In particular:
- Secure cryptographic device preparation shall be done securely
- Secure cryptographic device shall be securely stored and distributed

For Hard Tokens, the Subject Private Key is embedded within an encrypted data unit inside the HSM and thereafter loaded onto the smart card where it is decrypted. The Private Key is never available in clear text outside the HSM or the smart card. See 6.1.2.

d) The Subscriber is responsible for applying for Subject rekey (see 4) as needed. Any new Subject key SHALL be generated and distributed in the same manner as for the initial keys.

Certificate rekey require a new Certificate Application Key/Certificate distribution is handled in the same way as for the initial key/Certificate distribution.

**Subject key generation performed by the Subscriber**

e) Subject key generation SHALL be undertaken in a controlled environment under supervision by the Subject Sponsor.

f) The Private Key SHOULD be maintained under the Subject's sole control.

g) Subject keys MAY be generated and stored in software or on hardware token.

The Subscriber may generate the Private Key within an HSM acting as a Hard Token. The Subscriber must confirm and provide proof for the Private Key to be handled as Hard Token protected Key.

### 6.1.2 Private Key Delivery to Subscriber

For CA generated private Subject keys the following requirements applies;

a) The Subject's Private Key SHALL be delivered to the Subject such that the secrecy and integrity of the key is not compromised. If the CA or any of its designated RAs become aware that a Subject's Private Key has been communicated to an unauthorized person or an organization not affiliated with the subject, then the CA shall revoke all Certificates that include the Public Key corresponding to the communicated Private Key;

For Soft Tokens, the Private Key is delivered as an encrypted PKCS#12 file sent from Buypass to the e-mail address provided by the Certificate Applicant as part of the Certificate Application. The Distribution Key is distributed as described in 6.1.2 b).

For Hard Tokens, the Private Key is delivered as a smart card sent from Buypass by mail to the person identified as Subject Sponsor as part of the Certificate Application. The access to the Private Key is protected by a secret PIN. The PIN letter is sent to the Subject Sponsor in a mail separated in time from the smart card.

b) Encrypted software keys SHALL be distributed separately from the corresponding secret distribution (decryption) key.

For Soft Tokens, the Distribution Key is either sent in a PIN code letter to the person identified as Subject Sponsor or sent by SMS to a pre-authorized electronically authenticated Certificate Applicant.

Commercial services from the Norwegian Postal Service are used to ensure personal delivery when the Distribution Key is sent in a PIN code letter. However, when the PIN code letter is requested from a pre-authorized electronically authenticated Certificate Applicant, personal delivery is not used (see 3.2.2.1).

c) The CA SHALL ensure that the Subject is offered appropriate capabilities to maintain the Private Key under the Subject's sole control.

Through personal delivery of the secret Distribution Key for a Soft Token and the token itself for a Hard Token, Buypass ensures that the Private Key is protected during distribution.

For a Soft Token, the Private Key is imported from the PKCS#12 file and onto the Subscriber system where it is to be used. In this case, the Subscriber, through the Subject Sponsor, is responsible for ensuring appropriate Private Key protection.

Buypass does not have any control with Subscribers systems and their capabilities for Private Key protection once the Private Key is installed/made available to the target system.

For a Hard Token, the Private Key is always protected within the token itself and the Subscriber, through the Subject Sponsor, is responsible for ensuring appropriate protection of the token. The access to the Private Key requires a PIN distributed to the Subject Sponsor according to 6.4.1.

Buypass therefore explicitly, through the Subscriber Agreement, informs the Subscriber about its responsibility of applying appropriate Private Key protection. Buypass also imposes that the Subscriber records all individuals, systems and processes using the Private Key.

d) The CA shall delete all copies of a Subject Private Key after delivery of the Private Key to the Subject.

For Soft Tokens, neither the Private Key nor the PKCS#12 file is stored by Buypass after they have been sent by e-mail to the Subject Sponsor.

For Hard Tokens, no copy of the Private Key is held by Buypass after being loaded onto the token.

### 6.1.3 Public Key Delivery to Certificate Issuer

If the Subject's keys are generated by the Subscriber/Subject, the Public Key SHALL be delivered to the CA as part of a Certificate request. The Certificate request SHALL:

- authenticate the Subscriber or Subject Sponsor as the originator of the request
- contain proof that the requestor is in possession of the Private Key that corresponds to the Public Key in the request

For Subscriber generated Private Keys, the Public Key is delivered by the Subscriber as part of a PKCS#10 formatted Certificate Signing Request. The signature on the request provides proof of possession of the Private Key.

The authenticity of the request may be verified by the Certificate Applicant using electronic credentials issued by Buypass in order to submit the Certificate Application. Otherwise, the Public Key is included in the Certificate Application as described in 4.1.1 and its origin will be verified as a part of this.

### 6.1.4 CA Public Key Delivery to Relying Parties

a) CA signature verification (public) keys shall be available to Relying Parties in a manner that assures the integrity of the CA public key and authenticates its origin.

CA Public Keys are available through CA Certificates signed by a Root CA.

The Buypass Class 3 Root CA Certificate is pre-installed in common browsers and other relevant applications by the applicable software vendors.

The Buypass Class 3 Root CA G2 HT Certificate, Buypass Class 3 Root CA G2 ST Certificate, Buypass Class 3 CA G2 HT Business Certificate and Buypass Class 3 CA G2 ST Business Certificate are available in trust lists relevant for their purpose (e.g. EUTL and AATL).

The Issuing CA Certificates are included in the PKCS#12 file for Soft Tokens and also available through the AIA certificate extension.

The issuing CA and Root CA Certificates may also be downloaded from Buypass Web. All certificates' fingerprints are included on Buypass Web.

b) If a self-signed certificate is issued by the CA, the attributes of the certificate shall be compliant with the defined key usage as defined in Recommendation ITU-T X.509 [9]

Buypass issues Root Certificates as self-signed Certificates. The key usage of these Certificates is according to X.509 recommendation.

### 6.1.5 Key Sizes

**Root CA and CA keys**

a) CA key pair generation SHOULD be performed using an algorithm as specified in ETSI TS 119 312 [13] for the CA's signing purposes.

b) The selected key length and algorithm for CA signing key SHOULD be one which is specified in ETSI TS 119 312 [13] for the CA's signing purposes.

Buypass CA signature keys for Certificates are either RSA 2048 bits or RSA 4096 bits.

CA signatures on Certificates, CRLs and OCSP responses are based on these keys and using either SHA-256 or SHA-512 as hash algorithm.

The Buypass Class 3 Root CA key is RSA 4096 bits. Root CA signatures on CA certificates and CRLs for CA certificates are based on these keys and using SHA-256 as hash algorithm.

The Buypass Class 3 Root CA G2 HT and Buypass Class 3 Root CA G2 ST keys are RSA 4096 bits. Root CA signatures on CA Certificates and CRLs for CA Certificates are based on these keys and using SHA-512 as hash algorithm.

**Subject keys**

c) Subject keys SHALL be generated using an algorithm recognized as being fit for the uses identified in this Certificate Policy during the validity time of the Certificate, see [13].

d) Subject keys SHOULD be of a key length and for use with a public key algorithm as specified in ETSI TS 119 312 [13] for the purposes stated in this Certificate Policy during the validity time of the certificate.

For CA generated Private Keys, only RSA Subject keys are supported and the key size are at least 2048 bits for Soft Tokens and 2032 bits for Hard Tokens.

For Subscriber generated Private Keys, only RSA Subject keys are supported and the key size must be at least 2048 bits

### 6.1.6 Public Key Parameters Generation and Quality Checking

For RSA keys the CA SHALL confirm that the value of the public exponent is an odd number equal to 3 or more.

Upon reception of a Certificate Signing Request, Buypass verifies that the public exponent is an odd number equal to 3 or more.

Buypass checks whether the key is a Debian weak key or a ROCA weak key as described in the ROCA vulnerability identified as CVE-2017-15361. Any application for Certificates using such weak keys will be rejected.

### 6.1.7 Key Usage Purposes

**CA keys**

a) CA signing key(s) used for generating Certificates and/or issuing revocation status information, SHALL not be used for any other purpose.

The CA Private Key is used only to sign Certificates, CRLs and OCSP responses.

b) The use of the CA's Private Key shall be compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificate.

The CA Private Key is used to sign Certificates, CRLs and OCSP responses using algorithms and key lengths as specified in 6.1.5.

**Subject keys**

c) Key usage combinations SHALL be set according to [19] and compliant with [6] or [7] and [8].

For CA generated Private Keys, the Buypass Class 3 Enterprise Certificates comprises 2 different key pairs. One key pair is used for authentication and encryption and the other is used for electronic signature only.

For Subscriber generated Private Keys, authentication, encryption and electronic signature are combined within one key pair and Certificate.

The key usage combinations for these certificates are described in Buypass Class 3 Certificate and CRL profiles in [19].

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic Module Standards and Controls

The following requirements apply to the cryptographic module hosting the CA signing keys;

a) The CA private signing key SHALL be held and used within a secure cryptographic module which meets the requirements as defined in 6.1.1.1 d)

The Buypass Class 3 CA Private Keys are protected by and used within an HSM compliant to FIPS 140-2 level 3.

b) The CA SHALL ensure that CA Private Keys remain confidential and maintain their integrity.

See 6.2.1 a) and c)

c) Where the CA keys are stored in a dedicated key processing hardware module, access controls SHALL be in place to ensure that the keys are not accessible outside the hardware module.

The CA Private Keys are stored and protected by an HSM where access control mechanisms ensure that the Private Key is not accessible outside the module.

d) The CA SHALL ensure the security of the cryptographic module throughout its lifecycle. This includes protection against tampering during shipment and while stored.

Buypass maintains routines that cover the secure lifecycle management (generation, backup, cloning, archival, destruction) of all cryptographic modules containing the CA Private Key. All cryptographic modules containing copies of the CA Private Key is physically protected under dual control.

e) Signing operations using the CA Private Key SHALL only take place in a physically secured environment (see 5.1).

All signing operations that involve the CA Private Key is performed in Buypass' CA operations facility (see 5.1).

f) The secure cryptographic module shall be functioning correctly.

All HSMs are verified for correctness at startup.

g) The CA private signing keys stored on the CA's secure cryptographic module shall be destroyed upon modules retirement.

The CA private signing keys are never stored in an HMS. The keys are loaded and decrypted at time of use. When the HSM is retired, all keys necessary to decrypt CA private signing keys are destroyed.

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

See 6.1.1, 6.2.4 and 6.2.7

All physical access to cryptographic devices containing a copy of the CA Private Key requires dual control.

### 6.2.3 Private Key Escrow

No stipulations.

Buypass do not use Private Key escrow.

### 6.2.4 Private Key Backup

**CA key backup**

a) The CA private signing key SHALL be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

Only personnel in trusted roles are able to access cryptographic modules. See also 6.2.1 c). The physical access to the modules requires dual control.

b) For backup or cloning/redundancy purposes, the CA Private Key MAY be exchanged encrypted with another cryptographic device meeting the requirements in 6.1.1.1 b). This exchange is to take place using a trusted system in a physically secured environment (see 5.1) and under the control of three Security Officers.

The CA Private Keys are protected within an HSM, and unless used within the HSM the keys are encrypted using HSM enforced encryption and access control mechanisms.

c) When outside the secure cryptographic module the CA private signing key SHALL be protected in a way that ensures the same level of protection as provided by the secure cryptographic module.

Se 6.2.4 b)

d) Backup copies of the CA private signing keys SHALL be subject to the same or greater level of security controls as keys currently in use.

The CA Private Keys are protected within an HSM, and unless used within the HSM the keys are encrypted using HSM enforced encryption and access control mechanisms.

### 6.2.5 Private Key Archival

a) CA Private Keys SHALL be archived by the CA when they are no longer used.

Buypass archives CA Private Keys for at least 10 years after the CA Private Key is no longer in use.

b) The retention period SHALL be at least 10 years.

See 6.2.5 a)

c) Archived CA keys SHALL be subject to the same or greater level of security controls as keys currently in use.

See 6.2.4 d)

d) Archived CA keys SHALL never be put back into production.

CA Private Keys that has been archived will be kept in the archive until they are eventually destroyed.

e) All archived CA keys SHALL be destroyed at the end of the archive period using dual control in a physically secure site.

Buypass CA Private Keys that has been archived will be destroyed witnessed by three persons assuming a Security Officer role.

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

See 6.1.1.1 and 6.2.4

The CA Private Key is generated within a cryptographic module.

The CA Private Key may be copied from the cryptographic module where the key was generated and onto other cryptographic modules to support either Private Key backup or Private Key cloning. See 6.2.4 a)

### 6.2.7 Private Key Storage on Cryptographic Module

### 6.2.8 Activating Private Keys

**CA Private Key**

a) The Certificate signing keys SHALL only be activated and used within physically secure premises (see 5.1.1).

The CA Private Key is only activated and used within the CA Operations facility.

**Subject Private Key**

b) The Subscriber is responsible for ensuring that activation of the Subject Private Key uses Activation Data if required (see 6.4.1).

In case of CA generated Private Keys delivered as Hard Tokens, the Private Keys are protected within a smart card and access to the Private Key requires a PIN.

For all other Enterprise Certificates, the Subscriber must ensure that access to the Private Key is under Subscriber's sole control.

c) Dependent on support by the Subject system/application, the Subscriber MAY allow Private Key operations to occur using cached Activation Data.

### 6.2.9 Deactivating Private Keys

### 6.2.10 Destroying Private Keys

a) All copies of the CA private signing keys shall be destroyed at the end of their life cycle.

Buypass destroys all copies of the CA private signing keys at the end of their life cycle. One exception is for the archived CA private signing keys, see 6.2.5.

b) The CA SHALL ensure that all private signing keys stored on CA cryptographic hardware are completely destroyed under dual control upon device retirement except from those CA keys that are archived (see 6.2.5).

See 6.2.1 g)

No stipulations for Subject Private Keys.

### 6.2.11 Cryptographic Module Capabilities

## 6.3 Other aspects of key pair management

### 6.3.1 Public Key Archival

### 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the Certificate. The validity period is stated in the validity field of the Certificate.

**CA keys**

a) The CA SHALL ensure that CA private signing keys are not used beyond the validity period as defined in the corresponding CA certificate.

The signing key for Buypass Class 3 CA 3 has a lifetime of 20 years. The signing key for Buypass Class 3 Root CA has a lifetime of 30 years.

The signing keys for Buypass Class 3 CA G2 ST Business and Buypass Class 3 CA G2 HT Business have a lifetime of 20 years and the signing keys for Buypass Class 3 Root CA G2 HT and Buypass Class 3 Root CA G2 ST has a lifetime of 25 years.

The CA Private Keys will not be used beyond the validity period of the corresponding CA certificate. This is ensured by not signing certificates, CRLs or OCSP-responses with validity periods beyond the CA certificate validity period.

b) The CA Public Keys MAY be used for verifying signatures beyond the CA certificate validity period.

**Subject keys**

c) Subject Private Keys SHALL NOT be used beyond the Certificate validity period.

The Subject is committed to not use the Private Keys beyond the validity period of the corresponding Certificate.

d) Subject Public Keys MAY be used for verifying signatures beyond the Certificate validity period.

## 6.4 Activation data

### 6.4.1 Activation data generation and installation

a) CA Private Key Activation Data SHALL be generated by the CA using a random number generator and installed under the supervision of at least three Security Officers.

The CA Private Key is protected within an HSM and the access to the Key is protected by smart cards defining an operator card set. Different operator roles (i.e. System Administrator, Security Officer) may have different requirements regarding the number of cards required. The operator card sets was generated using the HSM during the CA Key ceremony under supervision of three Security Officers and an external auditor.

b) Activation Data protecting access to Subject Private Keys SHOULD be a strong password/PIN that cannot be easily guessed. Password protection MAY be omitted if reasonable security protection is applied to the computer itself that hosts the Private Key.

In case of CA generated Private Keys, for Hard Tokens the Subject Private Keys within the smart card are protected by a PIN which is at least 4 digits.

The initial PIN is generated randomly by Buypass and distributed to the Subject Sponsor by mail in a PIN letter together with a PIN Unlocking Key (PUK). The Subject Sponsor may set a new PIN code on receipt of the initial PIN.

c) When used, Subject Private Key Activation Data SHALL be generated and installed by the Subject Sponsor.

### 6.4.2 Activation data protection

a) The CA Private Key Activation Data SHALL be protected in a physically secured environment under dual control with at least one (1) Security Officer.

The CA Private Key Activation Data is implemented as cryptographic keys in smart cards integrated in the secure HSM environment. Access to the smart cards requires dual control.

b) Subject Private Key Activation Data SHALL be kept under the Subject's sole control.

In case of CA generated Private Keys, for Hard Tokens, the Subject Private Key Activation Data (i.e. the PIN) is kept inside the token and verified in the token when access to the Private Key is required. On unsuccessful verification a PIN retry counter is decremented.

The PIN retry counter is initially set to 3, and after 3 unsuccessful verifications, the PIN is locked, i.e. the access to the Subject Private Key inside the token is locked.

In order to unlock the PIN, the Subject Sponsor may present a PIN Unlocking Key (PUK). The PUK is distributed to the Subject Sponsor by mail and is under the Subject Sponsor's sole control. The PUK consists of 8 digits. When the PIN is unlocked, the PIN retry counter is reset to 3.

### 6.4.3 Other aspects of activation data

## 6.5 Computer security controls

### 6.5.1 Specific Computer Security Technical Requirements

a) The Computer Security Controls SHALL conform to the requirements defined by the policy for EU Qualified Certificates issued to legal persons (QCP-l) of ETSI EN 319 411-2 [17].

See 5 a)

b) Local network components (e.g. routers) SHALL be kept in a physically and logically secure environment and their configurations shall be periodically checked for compliance with the requirements specified by the CA.

See 5 a)

c) The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance

All accounts capable of directly causing certificate issuance are required to use a smartcard and PIN.

d) Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.

All certificates and associated information are protected from being added, deleted of modified.

e) Revocation status application SHALL enforce access control on attempts to modify revocation status information.

Revocation status information is protected from being modified.

f) Continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

Unauthorized and/or irregular attempts to access CA resources are monitored with triggering alarms.

### 6.5.2 Computer Security Rating

## 6.6 Life cycle technical controls

### 6.6.1 System development controls

The CA SHALL implement Life Cycle Security Controls according to best practice according to ISO/IEC 27002:2013 [6] and in compliance with Buypass Information Security Policy [3].

Systems development and maintenance activities are designed to maintain CA system integrity. Strict control is maintained over access to program source libraries. Formal change control procedures exist and are

followed for the implementation of software, scheduled software releases and emergency software fixes. See also 5 a)

### 6.6.2 Security management controls

### 6.6.3 Life cycle security controls

a) The Life Cycle Security Controls SHALL conform to the requirements defined by the policy for EU Qualified Certificates issued to legal persons (QCP-l) of ETSI EN 319 411-2 [17].

See 5 a)

b) Capacity demands shall be monitored and projections of future capacity requirements shall be made to ensure that adequate processing power and storage are available.

This is a continuous process based on real time monitoring and analysis of the performance.

## 6.7 Network security controls

a) The CA SHALL implement Network Security Controls according to best practice according to ISO/IEC 27002:2013 [11] and in compliance with Buypass Information Security Policy [3].

See 5 a)

b) The Network Security Controls SHALL conform to the requirements defined by the policy for EU Qualified Certificates issued to legal persons (QCP-l) of ETSI EN 319 411-2 [17].

See 5 a)

c) The CA SHALL maintain and protect all CA systems in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and high security zones.

Critical parts of the CA systems are protected within a High Security Zone with strict security requirements. The other CA systems are maintained and protected within secure zones.

d) The CA SHALL configure all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

For servers in the High Security Zone; accounts, applications and services not used are removed or disabled. Ports that are used are white listed in a firewall.

e) The CA SHALL grant access to secure zones and high security zones to only trusted roles.

Only persons in trusted roles have access to secure zones and the High Security Zone. For the High Security Zone two persons in trusted roles are required to access the servers.

f) The Root CA system SHALL be in a high security zone.

The Root CA system is maintained on a standalone, air gapped system which must be authorized by three Security Officers to operate.

## 6.8 Time-stamping

# 7 Certificate, CRL, and OCSP profiles

The Certificate, CRL and OCSP profiles SHALL be described in the Buypass Class 3 Certificate and CRL profiles [19] and the document SHALL be made publicly available on Buypass Web.

## 7.1 Certificate profile

The certificates shall meet the requirements, specified in Recommendation ITU-T X.509 [9] or IETF RFC 5280 [2].

Certificate profiles SHALL be in accordance with the SEID profile for Certificates issued to organizations [6].

### 7.1.1 Version Number(s)

### 7.1.2 Certificate Extensions

### 7.1.3 Algorithm Object Identifiers

### 7.1.4 Name Forms

### 7.1.5 Name Constraints

### 7.1.6 Certificate Policy Object Identifier

### 7.1.7 Usage of Policy Constraints Extension

### 7.1.8 Policy Qualifiers Syntax and Semantics

### 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

## 7.2 CRL profile

The CRL shall be as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 [9] or IETF 5280 [2].

### 7.2.1 Version number(s)

### 7.2.2 CRL and CRL entry extensions

## 7.3 OCSP profile

The OCSP profile SHALL conform to the specifications contained in RFC 6960 [18].

### 7.3.1 Version number(s)

### 7.3.2 OCSP extensions

# 8 Compliance audit and other assessments

## 8.1 Frequency or circumstances of assessment

The CA SHALL be audited once per calendar year for compliance with the practices and procedures set forth in the Certification Practice Statement for Buypass Class 3 Enterprise Certificates [21].

Buypass is audited annually for conformance to ETSI EN 319 401 [14], ETSI TS 319 411-1 [16] and ETSI EN 319 411-2 [17].

As a result, Buypass has received compliance certificates that confirms that Buypass issues Certificates according to the standards mentioned above. The compliance certificates are renewed annually.

Buypass Enterprise Certificates are covered by the compliance certificate identified as ETS 018 and as EU Qualified Certificates for electronic seal is covered by the compliance certificate identified as ETS 053.

## 8.2 Identity/qualifications of assessor

The CA's audit SHALL be performed by a Qualified Auditor.

Buypass uses an auditor that is accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403.

## 8.3 Topics covered by assessment

The audit report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in 1.2. The CA SHALL make the audit report publicly available.

The compliance certificates include a statement for each of the policy identifiers used in the Certificates, defining which ETSI policies being used for verifying compliance.

The latest versions of the compliance certificates are published on Buypass Web.

## 8.4 Actions taken as a result of deficiency

## 8.5 Communication of results

## 8.6 Self-Audits

During the period in which the CA issues Certificates, the CA SHALL monitor adherence to its Certificate Policy,Certification Practice Statement and these Requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Buypass performs self audits on a quarterly basis of approximately one percent of the Certificates. Samples are selected randomly.

# 9 Other business and legal matters

## 9.1 Fees

### 9.1.1 Certificate issuance or renewal fees

The fees for services provided by Buypass in respect to Buypass Class 3 Enterprise Certificates SHALL be published on Buypass Web. These fees are subject to change, and any such changes SHALL be notified before the fees become effective.

The service fees charged by Buypass for Buypass Class 3 Enterprise Certificates are published on Buypass Web.

### 9.1.2 Certificate access fees

### 9.1.3 Revocation or status information access fees

### 9.1.4 Fees for other services

### 9.1.5 Refund policy

## 9.2 Financial responsibility

The financial responsibility requirements defined in this section are reflected in the applicable Subscriber Agreements and Relying Party Agreements.

### 9.2.1 Insurance coverage

### 9.2.2 Other assets

### 9.2.3 Insurance or warranty coverage for end-entities

## 9.3 Confidentiality of business information

### 9.3.1 Scope of confidential information

Information about Subscribers that are not evident from the Certificates themselves SHALL be considered confidential.

The following information is not considered confidential/private;

- Certificates
- Certificate revocation status information

All other information about Subscribers, Subscriber Representatives and their use of Buypass services will be treated as confidential/private by Buypass. Buypass handles private information according to [22], [27] and [28].

### 9.3.2 Information not within the scope of confidential information

### 9.3.3 Responsibility to protect confidential information

## 9.4 Privacy of personal information

### 9.4.1 Privacy plan

a) The CA SHALL provide evidence of how they meet applicable data protection legislation within their registration process.

Buypass complies with the Norwegian law in all matters concerning data protection.

b) The CA's verification policy SHALL only require the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.

All identity information captured regarding Certificates (see 3.2) are required to satisfy the requirements for their intended use.

c) Registered Subscriber information MAY be disclosed to the Subscriber upon request.

Registered Subscriber information will be disclosed to the respective Subscriber only after having received an authenticated request from an Authorized Subscriber Representative.

### 9.4.2 Information treated as private

### 9.4.3 Information not deemed private

### 9.4.4 Responsibility to protect private information

a) The confidentiality and integrity of registration data shall be protected, especially when exchanged with the Subscriber/Subject or between distributed CA system components

See 9.3.1

b) Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities

See 9.4.6

### 9.4.5 Notice and consent to use private information

### 9.4.6 Disclosure pursuant to judicial or administrative process

Buypass SHALL have the right to release information that is considered confidential to law enforcement officials in compliance with Norwegian law.

Buypass complies with the Norwegian law in all matters concerning release of confidential information to law enforcement officials.

### 9.4.7 Other information disclosure circumstances

## 9.5 Intellectual property rights

a) Key pairs corresponding to Buypass CA Certificates SHALL be the property of Buypass. Key pairs corresponding to Certificates SHALL be the property of the respective Subscriber of those Certificates.

b) Buypass SHALL retain all intellectual property rights in and to the Certificates and revocation information that it issues except for any information that is supplied by a Subscriber and that is included in a Certificate, which information SHALL remain the property of the Subscriber. Buypass and Subscribers SHALL grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the applicable Relying Party Agreement.

c) A Subscriber SHALL retain 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 Subscriber.

d) Buypass SHALL retain all Intellectual Property Rights in and to the Certificate Policy [20] and the Certification Practice Statement [21].

## 9.6 Representations and warranties

Buypass operates as both the CA and RA for all Certificates issued under the Certificate Policy [20] and thereby fulfills all CA and RA obligations in this section.

### 9.6.1 CA Representations and Warranties

The CA SHALL provide the following core CA/RA services:

- registration service
- certificate generation service
- dissemination service
- revocation management service
- revocation status service

- subject device provision service

Buypass offers all the above CA/RA services. The subject device provision service is relevant for Hard Tokens when Buypass generates the Private Key only.

In addition, Buypass provides a Norwegian and English speaking customer support service (Buypass Kundeservice) that can be reached by phone and by e-mail.

The CA MAY provide a Subject Key Generation and Subject Key Provision Service.

Buypass provides both a Subject Key Generation service and a Subject Key Provision Service.

The Subject Private Keys can be distributed as Soft Token or Hard Token based on Subscriber's choice. The Soft Token is a PKCS#12 file encrypted with a secret Distribution Key. The Hard Token is a smart card where the access to the Private Keys is protected by a secret PIN.

Buypass also accepts Enterprise Certificate requests based on Subscriber generated Private Keys. If the Private Keys are generated and protected in a Hardware Security Module (HSM) the Certificates issued are Hard Token Certificates. If the Private Keys are generated and protected outside an HSM the Certificates issued are Soft Token Certificates.

The CA MAY subcontract one or more of the offered services, or parts of these.

Buypass use commercial services from the Norwegian Postal Service for secure distribution of Distribution Keys for Soft Tokens or the token itself for Hard Tokens in case of CA generated keys.

For Subscriber generated keys, the same services may be used for secure distribution of an Authorization Code before Certificate issuance.

The CA SHALL be responsible for providing its CA/RA services in conformance with the Certificate Policy for Buypass Class 3 Enterprise Certificates [20] and consistent with the Certification Practice Statement for Buypass Class 3 Enterprise Certificates [21], even when functionality is undertaken by sub-contractors.

See 9.6.1

The CA SHALL warrant that the identity of the Subscriber (organization that the Subject represents) that appears in an issued Certificate is accurate and correct at the time of issuance.

To avoid any conflicts of interests, the Subscriber and CA organization entity SHALL be separate entities. The only exception is the organization running all or part of the RA tasks subscribing a certificate for itself or persons identified in association with it (as a subject), and for which the exception is stated in the CA's policies.

Buypass as a CA may issue Enterprise Certificates to Buypass as a Subscriber. Since Buypass also performs all RA tasks for these Certificates, this is an acceptable exception from this requirement conflict of interest.

The CA SHALL warrant that an issued Certificate is linked to one (1) unique organization registered in a QGR.

The CA SHALL warrant that the Subscriber is in possession of the Subject Private Key that corresponds to the Public Key in that Certificate. If the Subject's Private Key is generated by the CA, the CA SHALL provide the Subject with means to protect the Private Key.

The CA SHALL ensure timely publication of revocation information in accordance with the publication requirements defined in this document.

The CA SHALL provide the capability to allow third parties to check and test all the Certificate types that the CA issues.

Buypass provides test certificates for all types of Enterprise Certificates

Any test certificates should clearly indicate that they are for testing purposes (e.g. by the subject name).

All test certificates are issued by test CAs where the CA name clearly indicates that this is for test purposes (e.g. Buypass Class 3 Test4 CA 3).

### 9.6.2 RA Representations and Warranties

Buypass SHALL operate the RA services, or parts of these, that has not been subcontracted.
The RA SHALL:

- receive Certificate Applications from Subscribers, both initial applications (see 4.1.1) and rekey applications (see 4.7)
- verify all information submitted by Subscribers, both for initial applications and for rekey applications and if such verification is successful, submit a request to the CA for the issuance of a Buypass Class 3 Enterprise Certificate
- receive and verify requests from Subscribers for the revocation of Buypass Class 3 Enterprise Certificates, and if the verification of a revocation request is successful, submit a request to the CA for the revocation of such Certificate
- notify Subscribers that a Buypass Class 3 Enterprise Certificate has been issued to them

notify Subscribers that a Buypass Class 3 Enterprise Certificate issued to them has been suspended, revoked or will soon expire

### 9.6.3 Subscriber Representations and Warranties

The Subscriber SHALL fulfil all obligations of the Subscriber Agreement. The Subscriber SHALL:

- submit accurate and complete information to the CA in accordance with the requirements in the Certification Practice Statement for Buypass Class 3 Enterprise Certificates [21]
- maintain correct information about the Subscriber and Subject, and notify the RA or CA of any changes to this information
- notify the RA or CA if any information in the Certificate is incorrect
- request the Certificate to be revoked when a valid revocation reason exists (see 4.9.1.1)
- inform the RA whenever an Authorized Subscriber Representative no longer is authorized to represent the Subscriber
- ensure that the Private Keys and Certificates are only used in accordance with any limitations notified to the Subscriber
- if the Subscriber generates the Private Key, ensure that the key generation and the Private Key satisfies the requirements in 6.1.1.3 and 6.1.5
- If the Subscriber generates the Private Key as a Hard Token, the Private Key must be generated and used only in a Hardware Security Module (HSM)
- exercise reasonable care to avoid unauthorized use of the Subject's Private Keys
- the use of the Private Key is immediately and permanently discontinued (except for key decipherment) if the Private Key is compromised or the Certificate is revoked
- in the case of being informed that the CA has been compromised, ensure that the Private Key is no longer used
- inform Subject Sponsors of all obligations applicable to the Subject

ensure that the use of the Private Key-is under Subscriber's sole control by recording all entities that have access to and use the Private Key, this includes individuals, systems and processes

### 9.6.4 Relying Party Representations and Warranties

A Relying party is solely responsible for deciding whether or not to rely on Certificates issued under the Certificate Policy for Buypass Class 3 Enterprise Certificates [20].

When validating an Electronic Signature or Electronic Seal, the Relying Party SHALL take into consideration all information in the Certificate, this Policy and obey best practices for validating signatures (see for example [21]).

The Relying party SHALL

- restrict reliance on Buypass Class 3 Enterprise Certificates to the purposes for those Certificates as defined by 1.4
- acknowledge applicable terms, conditions, warranties and liability caps as defined in 9.8
- rely on a Buypass Class 3 Enterprise Certificate only if such reliance is reasonable in the circumstances, including determining whether such reliance is reasonable given the nature of the security and trust provided by a Buypass Class 3 Enterprise Certificate and the value of any transaction that may involve the use of a Buypass Class 3 Enterprise Certificate
- consult the most recent revocation status information in order to establish whether any of the Certificates in the certification path have been revoked or suspended
- verify Buypass Class 3 Enterprise Certificates, including use of revocation services, in accordance with best practice certification path validation as defined by RFC 5280 [2]

If it is not possible to perform all of the above, the Relying Party SHALL NOT trust the Certificate.

### 9.6.5 Representations and Warranties of Other Participants

The CA SHALL have a properly documented agreement and contractual relationship in place where the provisioning of services (see 9.6.1) involves subcontracting, outsourcing or other third party arrangements.

The Subcontractor SHALL fulfil all obligations as defined by the respective subcontractor agreement, including the implementation of any controls required by the CA.

The services provided by the Norwegian Postal Service for secure distribution are commercial services with security controls, liability and a quality of service that are not subject to special regulations from Buypass.

## 9.7 Disclaimers of warranties

Issuance of Certificates in accordance with the Certificate Policy [20] SHALL NOT make the CA an agent, fiduciary, trustee, or other representative of Subscribers or Relying Parties

## 9.8 Limitations of liability

To the extent permitted by Norwegian law, Subscriber Agreements and Relying Party Agreements SHALL limit the CA's liability.

The CA's liability to the Subscriber or Relying Party for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on Buypass Class 3 Enterprise Certificates SHALL be limited as follows:

- For EU Qualified Certificates: 2.000 EUR (two thousand Euros) per Subscriber or Relying Party concerning a specific Certificate or any services provided in respect to this Certificate.

- For non EU Qualified Certificates: 1.000 EURO (one thousand Euros) per Subscriber or Relying Party concerning a specific Certificate or any services provided in respect to this Certificate.
  The total liability for damages for a specific Relaying Party concerning all Certificates or any services in respect to these Certificates is limited to 5000 EUR (five thousand Euros).

Limitations of liability SHALL include an exclusion of indirect, special, and consequential damages.

Relying Parties and Subscribers MAY buy into coverage schemes that will improve Relying Party protection.

Any Relying Party that requires further economic liabilities than described above need to enter into a special agreement with Buypass.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements SHALL include a force majeure clause protecting Buypass.

## 9.9 Indemnities

### 9.9.1 Indemnification by Cas

### 9.9.2 Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers SHALL indemnify and hold Buypass harmless from and against any and all liabilities, losses, costs, expenses, damages, claims and settlement amounts arising out of or relating to any reliance by a Relying Party on any Buypass Class3 Enterprise Certificate or any service provided in respect to Buypass Class 3 Enterprise Certificates for:

- The Subscriber's failure to perform the obligations of a Subscriber as defined in 9.6.3,
- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's Private Key, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's Private Key, or
- The Subscriber's use of a name (including without limitation within a common name) that infringes upon the Intellectual Property Rights of a third party.

### 9.9.3 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Parties SHALL indemnify and hold Buypass harmless from and against any and all liabilities, losses, costs, expenses, damages, claims and settlement amounts arising out of or relating to any reliance by a Relying Party on any Buypass Class 3 Enterprise Certificate or any service provided in respect to Buypass Class 3 Enterprise Certificates for:

- The Relying Party's failure to perform the obligations of a Relying Party as defined in 9.6.4.

The applicable Subscriber Agreement MAY include additional indemnity obligations.

## 9.10 Term and termination

### 9.10.1 Term

### 9.10.2 Termination

### 9.10.3 Effect of termination and survival

## 9.11 Individual notices and communications with participants

## 9.12 Amendments

### 9.12.1 Procedure for amendment

a) There SHALL be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the CP.

Buypass Policy Board MAY amend the Certificate Policy [20] or the Certification Practice Statement [21] at its own discretion.

b) A risk assessment SHOULD be carried out to evaluate business requirements and determine the security requirements to be included in the CP for the stated community and applicability.

Risk assessment is conducted regularly and may have effect on the security requirements in the CP.

c) CPs SHOULD be approved and modified in accordance with a defined review process, including responsibilities for maintaining the CP.

The CP and CPS are modified and approved by Buypass Policy Board in accordance with a defined review process. See also 1.5.4.

### 9.12.2 Notification mechanism and period

Minor changes to layout and text MAY be amended without further notice.

Buypass MAY change any part of the Certificate Policy [20] or the Certification Practice Statement [21] with 15 days advance notice.

Any change that may materially influence users of the Certificate Policy [20] or the Certification Practice Statement [21] SHALL be published on Buypass Web.

Users that are influenced by a change MAY comment upon it. Whether or not comments are honoured, SHALL solely be for Buypass Policy Board to decide. A change in the Certificate Policy [20] or the Certification Practice Statement [21] that is amended SHALL be subject to a new advance notice.

Modifications to either the Certificate Policy [20] or the Certification Practice Statement [21] that in the judgment of Buypass will have little or no impact on Subscribers and Relying Parties, may be made with no change in version number and no prior notification to Subscribers and Relying Parties. Such changes shall become effective immediately upon publication on Buypass Web.

In the event that Buypass makes a significant modification to either the Certificate Policy [20] or the Certification Practice Statement [21] the respective document version number will be updated accordingly. In this case a change notification will be published on the Buypass web no later than 15 days before the new document version becomes effective.

Any change that may have a major impact for existing Subscribers and/or Relying Parties will be notified explicitly in due time.

This gives Subscribers and Relying Parties a chance to comment upon the change. Unless a Subscriber ceases to use or requests revocation of such Subscriber's Certificate(s) prior to the date on which an updated document version becomes effective, such Subscriber shall be deemed to have consented to the modification.

### 9.12.3 Circumstances under which OID must be changed

## 9.13 Dispute resolution provisions

Complaints from customers or other parties in respect to any Buypass Class 3 Enterprise Certificate or any services provided in respect to any Buypass Class 3 Enterprise Certificate SHALL be handled without any unreasonable delay. The complaining party SHALL receive an answer to the complaint within 14 calendar days from the reception of the complaint; if it is not possible to complete the handling of the complaint within that time, the complainer shall receive a preliminary answer, if possible with an indication as to how much more time will be needed to provide an answer.

In case of a dispute arising out of or in respect to any Buypass Class 3 Enterprise Certificate or any services provided in respect to any Buypass Class 3 Enterprise Certificate the parties SHALL try to settle the dispute through negotiations and conciliation. If the dispute is not resolved within 3 months from the commencement

of the conciliatory process, each party has the right to bring the dispute to a Norwegian court for settlement. Oslo District Court shall be the exclusive first instance venue for all such disputes.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements MAY contain a dispute resolution clause.

## 9.14 Governing law

The laws of the country of Norway SHALL govern the construction, validity, interpretation, enforceability and performance of the Certificate Policy [20], the Certification Practice Statement [21], all related Subscriber Agreements and all related Relying Party Agreements

## 9.15 Compliance with applicable law

## 9.16 Miscellaneous provisions

The interpretation and enforcement requirements in this section are reflected in the applicable Subscriber Agreements.

### 9.16.1 Entire Agreement

### 9.16.2 Assignment

### 9.16.3 Severability

**Severability**
In the event that a clause or provision of the Certificate Policy [20] or the Certification Practice Statement [21] is held to be unenforceable by a court of law, the remainder of the respective Certificate Policy or Certification Practice Statement SHALL remain valid.

**Survival**
Subscribers and Relying Parties SHALL be bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates, also upon termination or expiration of the Certificate Policy [20], the Certification Practice Statement [21], any Subscriber Agreements and any Relying Party Agreements.

**Merger**
The Rights and Obligations of Buypass as CA/RA MAY be modified only in a writing signed or authenticated by a duly authorized representative of Buypass.

**Notice**
Any notice to be given by a Subscriber, Applicant, or Relying Party to Buypass under the Certificate Policy [20], the Certification Practice Statement [21], a Subscriber Agreement, or a Relying Party Agreement SHALL be given in writing (e-mail, post, courier) to the contact point specified in 1.5.2.

Any notice to be given by Buypass under Subscription Agreement SHALL be given in writing (by e-mail, by post or by courier) to the last address or email address for the Subscriber on file with Buypass.

### 9.16.4 Enforcement (attorneys' fees and waiver of rights)

### 9.16.5 Force Majeure

## 9.17Other provisions