Version: 6.0
Document date: 16.11.2020
Effective date: 01.12.2020

PUBLIC

Certification Practice Statement

Buypass Class 3 Person Qualified Certificates

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

www.buypass.no | 22 70 13 00

TABLE OF CONTENTS

1 Introduction 8

1.1 Overview 8
1.1.1 CA hierarchy 8
1.2 Document name and Identification 8
1.2.1 Revisions 9
1.3 PKI Participants 9
1.3.1 Certification Authorities 10
1.3.2 Registration Authorities 10
1.3.3 Subscribers 10
1.3.4 Relying Parties 10
1.3.5 Other Participants 10
1.4 Certificate Usage 10
1.4.1 Primary Certificate Purposes 10
1.4.2 Secondary Certificate Purposes 10
1.4.3 Excluded Certificate Purposes 10
1.5 Policy administration 10
1.5.1 Organization Administering the Document 10
1.5.2 Contact Person 10
1.5.3 Person Determining CPS suitability for the policy 10
1.5.4 CPS approval procedures 11
1.6 Definitions and acronyms 11
1.6.1 Definitions 11
1.6.2 References 14
1.6.3 Conventions 15

2 Publication and repository responsibilities 15

2.1 Publication of information 15
2.2 Time or frequency of publication 15
2.3 Access controls on repositories 15

3 Identification and authentication 16

3.1 Naming 16
3.1.1 Types of names 16
3.1.2 Need for names to be meaningful 16
3.1.3 Anonymity or pseudonymity of subscribers 16
3.1.4 Rules for interpreting various name forms 16
3.1.5 Uniqueness of names 16
3.1.6 Recognition, authentication, and role of trademarks 16
3.2 Initial identity validation 16
3.2.1 Method to Prove Possession of Private Key 16
3.2.2 Authentication of Organization Identity 17
3.2.3 Authentication of Individual Identity 18
3.2.4 Non-verified Subscriber Information 19
3.2.5 Validation of Authority 19
3.2.6 Criteria for Interoperation or Certification 20
3.3 Identification and authentication for re-key requests 20
3.3.1 Identification of Subject 20
3.3.2 Authentication of Subject 20
3.3.3 Identification and authentication of Subscriber and Subscriber representatives 21
3.3.4 Proof of possession of Private Key 21
3.4 Identification and authentication for revocation request 22

4 Certificate life-cycle operational requirements 22

4.1 Certificate Application 22
4.1.1 Who Can Submit a Certificate Application 22
4.1.2 Enrollment Process and Responsibilities 24
4.2 Certificate application processing 24
4.2.1 Performing Identification and Authentication Functions 24
4.2.2 Approval or Rejection of Certificate Applications 25
4.2.3 Time to Process Certificate Applications 25
4.3 Certificate issuance 25
4.3.1 CA Actions during Certificate Issuance 25
4.3.2 Notification of Certificate Issuance 25
4.4 Certificate acceptance 25
4.4.1 Conduct constituting certificate acceptance 26
4.4.2 Publication of the certificate by the CA 26
4.4.3 Notification of certificate issuance by the CA to other entities 26
4.5 Key pair and certificate usage 26
4.5.1 Subscriber private key and certificate usage. 26
4.5.2 Relying party public key and certificate usage 26
4.6 Certificate renewal 26
4.6.1 Circumstance for certificate renewal 26
4.6.2 Who may request renewal 26
4.6.3 Processing certificate renewal requests 26
4.6.4 Notification of new certificate issuance to subscriber 27
4.6.5 Conduct constituting acceptance of a renewal certificate 27
4.6.6 Publication of the renewal certificate by the CA 27
4.6.7 Notification of certificate issuance by the CA to other entities 27
4.7 Certificate re-key 27
4.7.1 Circumstance for certificate re-key 27
4.7.2 Who may request certification of a new public key 27
4.7.3 Processing certificate re-keying requests 27
4.7.4 Notification of new certificate issuance to subscriber 27
4.7.5 Conduct constituting acceptance of a re-keyed certificate 27
4.7.6 Publication of the re-keyed certificate by the CA 27
4.7.7 Notification of certificate issuance by the CA to other entities 27
4.8 Certificate modification 27
4.8.1 Circumstance for certificate modification 27
4.8.2 Who may request certificate modification 27
4.8.3 Processing certificate modification requests 27
4.8.4 Notification of new certificate issuance to subscriber 27
4.8.5 Conduct constituting acceptance of modified certificate 27
4.8.6 Publication of the modified certificate by the CA 28
4.8.7 Notification of certificate issuance by the CA to other entities 28
4.9 Certificate revocation and suspension 28
4.9.1 Circumstances for Revocation 29
4.9.2 Who Can Request Revocation 29
4.9.3 Procedure for Revocation Request 30
4.9.4 Revocation Request Grace Period 30
4.9.5 Time within which CA Must Process the Revocation Request 30
4.9.6 Revocation Checking Requirement for Relying Parties 31
4.9.7 CRL Issuance Frequency 31
4.9.8 Maximum Latency for CRLs 31
4.9.9 On-line Revocation/Status Checking Availability 31
4.9.10 On-line Revocation Checking Requirements 31

4.9.11 Other Forms of Revocation Advertisements Available 31
4.9.12 Special Requirements Related to Key Compromise 32
4.9.13 Circumstances for Suspension 32
4.9.14 Who Can Request Suspension 32
4.9.15 Procedure for Suspension Request 32
4.9.16 Limits on Suspension Period 32
4.10 Certificate status services 32
4.10.1 Operational Characteristics 32
4.10.2 Service Availability 32
4.10.3 Optional Features 32
4.11 End of subscription 32
4.12 Key escrow and recovery 32
4.12.1 Key escrow and recovery policy and practices 32
4.12.2 Session key encapsulation and recovery policy and practices 32

5 Management, operational, and physical controls 33

5.1 Physical security Controls 33
5.1.1 Site location and construction 33
5.1.2 Physical access 34
5.1.3 Power and air conditioning 34
5.1.4 Water exposures 35
5.1.5 Fire prevention and protection 35
5.1.6 Media storage 35
5.1.7 Waste disposal 35
5.1.8 Off-site backup 35
5.2 Procedural controls 35
5.2.1 Trusted Roles 35
5.2.2 Number of Individuals Required per Task 35
5.2.3 Identification and Authentication for Trusted Roles 36
5.2.4 Roles Requiring Separation of Duties 36
5.3 Personnel controls 36
5.3.1 Qualifications, Experience, and Clearance Requirements 36
5.3.2 Background Check Procedures 37
5.3.3 Training Requirements and Procedures 37
5.3.4 Retraining Frequency and Requirements 37
5.3.5 Job Rotation Frequency and Sequence 37
5.3.6 Sanctions for Unauthorized Actions 37
5.3.7 Independent Contractor Controls 38
5.3.8 Documentation Supplied to Personnel 38
5.4 Audit logging procedures 38
5.4.1 Types of Events Recorded 38
5.4.2 Frequency for Processing and Archiving Audit Logs 39
5.4.3 Retention Period for Audit Logs 40
5.4.4 Protection of Audit Log 40
5.4.5 Audit Log Backup Procedures 40
5.4.6 Audit Log Accumulation System (internal vs. external) 40
5.4.7 Notification to Event-Causing Subject 40
5.4.8 Vulnerability Assessments 41
5.5 Records archival 41
5.5.1 Types of Records Archived 41
5.5.2 Retention Period for Archive 41
5.5.3 Protection of Archive 41
5.5.4 Archive Backup Procedures 41
5.5.5 Requirements for Time-stamping of Records 41

5.5.6 Archive Collection System (internal or external) 41
5.5.7 Procedures to Obtain and Verify Archive Information 41
5.6 Key changeover 42
5.7 Compromise and disaster recovery 42
5.7.1 Incident and Compromise Handling Procedures 42
5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted 42
5.7.3 Recovery Procedures After Key Compromise 43
5.7.4 Business Continuity Capabilities after a Disaster 43
5.8 CA or RA termination 43

6 Technical security controls 44

6.1 Key pair generation and installation 44
6.1.1 Key Pair Generation 44
6.1.2 Private Key Delivery to Subscriber 46
6.1.3 Public Key Delivery to Certificate Issuer 46
6.1.4 CA Public Key Delivery to Relying Parties 47
6.1.5 Key Sizes 47
6.1.6 Public Key Parameters Generation and Quality Checking 48
6.1.7 Key Usage Purposes 48
6.2 Private Key Protection and Cryptographic Module Engineering Controls 48
6.2.1 Cryptographic Module Standards and Controls 48
6.2.2 Private Key (n out of m) Multi-person Control 50
6.2.3 Private Key Escrow 50
6.2.4 Private Key Backup 50
6.2.5 Private Key Archival 50
6.2.6 Private Key Transfer into or from a Cryptographic Module 51
6.2.7 Private Key Storage on Cryptographic Module 51
6.2.8 Activating Private Keys 51
6.2.9 Deactivating Private Keys 51
6.2.10 Destroying Private Keys 52
6.2.11 Cryptographic Module Capabilities 52
6.3 Other aspects of key pair management 52
6.3.1 Public Key Archival 52
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 52
6.4 Activation data 52
6.4.1 Activation data generation and installation 52
6.4.2 Activation data protection 53
6.4.3 Other aspects of activation data 54
6.5 Computer security controls 54
6.5.1 Specific Computer Security Technical Requirements 54
6.5.2 Computer Security Rating 54
6.6 Life cycle technical controls 54
6.6.1 System development controls 54
6.6.2 Security management controls 55
6.6.3 Life cycle security controls 55
6.7 Network security controls 55
6.8 Time-stamping 56

7 Certificate, CRL, and OCSP profiles 56

7.1 Certificate profile 56
7.1.1 Version Number(s) 56
7.1.2 Certificate Extensions 56
7.1.3 Algorithm Object Identifiers 56
7.1.4 Name Forms 56

7.1.5 Name Constraints 56
7.1.6 Certificate Policy Object Identifier 56
7.1.7 Usage of Policy Constraints Extension 56
7.1.8 Policy Qualifiers Syntax and Semantics 56
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 56
7.2 CRL profile 56
7.2.1 Version number(s) 56
7.2.2 CRL and CRL entry extensions 56
7.3 OCSP profile 56
7.3.1 Version number(s) 56
7.3.2 OCSP extensions 56

8 Compliance audit and other assessments 57

8.1 Frequency or circumstances of assessment 57
8.2 Identity/qualifications of assessor 57
8.3 Topics covered by assessment 57
8.4 Actions taken as a result of deficiency 57
8.5 Communication of results 57
8.6 Self-Audits 57

9 Other business and legal matters 57

9.1 Fees 57
9.1.1 Certificate issuance or renewal fees 57
9.1.2 Certificate access fees 58
9.1.3 Revocation or status information access fees 58
9.1.4 Fees for other services 58
9.1.5 Refund policy 58
9.2 Financial responsibility 58
9.2.1 Insurance coverage 58
9.2.2 Other assets 58
9.2.3 Insurance or warranty coverage for end-entities 58
9.3 Confidentiality of business information 58
9.3.1 Scope of confidential information 58
9.3.2 Information not within the scope of confidential information 58
9.3.3 Responsibility to protect confidential information 58
9.4 Privacy of personal information 58
9.4.1 Privacy plan 58
9.4.2 Information treated as private 59
9.4.3 Information not deemed private 59
9.4.4 Responsibility to protect private information 59
9.4.5 Notice and consent to use private information 59
9.4.6 Disclosure pursuant to judicial or administrative process 59
9.4.7 Other information disclosure circumstances 59
9.5 Intellectual property rights 59
9.6 Representations and warranties 59
9.6.1 CA Representations and Warranties 60
9.6.2 RA Representations and Warranties 61
9.6.3 Subscriber Representations and Warranties 61
9.6.4 Relying Party Representations and Warranties 62
9.6.5 Representations and Warranties of Other Participants 62
9.7 Disclaimers of warranties 63
9.8 Limitations of liability 63
9.9 Indemnities 63
9.9.1 Indemnification by Cas 63

9.9.2 Indemnification by Subscribers 63
9.9.3 Indemnification by Relying Parties 64
9.10 Term and termination 64
9.10.1 Term 64
9.10.2 Termination 64
9.10.3 Effect of termination and survival 64
9.11 Individual notices and communications with participants 64
9.12 Amendments 64
9.12.1 Procedure for amendment 64
9.12.2 Notification mechanism and period 64
9.12.3 Circumstances under which OID must be changed 65
9.13 Dispute resolution provisions 65
9.14 Governing law 65
9.15 Compliance with applicable law 65
9.16 Miscellaneous provisions 65
9.16.1 Entire Agreement 65
9.16.2 Assignment 65
9.16.3 Severability 65
9.16.4 Enforcement (attorneys' fees and waiver of rights) 66
9.16.5 Force Majeure 66
9.17 Other provisions 66

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

This document contains the Certification Practice Statement for Buypass Class 3 Qualified Certificates issued to natural persons. The term ‘Qualified Certificate’ is used synonymously with ‘Qualified Certificates issued to natural persons’ in this document.

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

Buypass Class 3 Qualified Certificates are issued to individuals registered in the National Population Register.

The certificates issued under this policy are Qualified Certificates according to Norwegian law and satisfies the requirements for eID High according to ‘Selvdeklarasjonsforskriften” [20].

The Certificates are also EU Qualified Certificates issued to natural persons according to Regulation (EU) No 910/2014 [19]. The Certificate Policy for Buypass Class 3 Qualified Certificates [17] is in this case aligned with the Qualified Certificate Policy for natural persons (QCP-n – see [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 Qualified Certificates issued to natural person comprises two different hierarchies:

1. The Buypass Class 3 CA hierarchy and
2. The Buypass Class 3 G2 HT 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 Qualified Certificates as specified in this document and Enterprise certificates.

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 as specified in this document, while Buypass Class 3 CA G2 HT Business issues Enterprise Certificates.

1.2 Document name and Identification

The Certificate Policy for Buypass Class 3 Qualified Certificates has been provided the following Certificate Policy Identifiers / 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

Relying Parties SHALL recognize a particular Certificate as having been issued under [17] by inspecting the Certificate Policies extension field of the Certificate, which then SHALL hold one of the policy OIDs above.

Both policies specified above are based on the QCP-n certificate policy for EU qualified certificates issued to natural persons [14]. All requirements that applies to the QCP-n certificate policy also applies to the policies specified above. Both policies require a secure cryptographic device termed a Signature Creation Device (SCD) in this document.

Buypass Class 3 CA 3 also issues certificates under the following Certificate Policies / OIDs:

- Certificate Policy for Buypass Class 3 Enterprise Certificates
  - OID 2.16.578.1.26.1.3.2 (Soft Token)
  - OID 2.16.578.1.26.1.3.5 (Hard Token)

1.2.1 Revisions

Version	Document Date	Description/Change
1.0	10.05.2005	Approved by Buypass Policy Board
2.0	29.04.2011	Approved by Buypass Policy Board
3.0	28.04.2014	Minor changes
4.0	20.04.2016	Included Buypass Class 3 Qualified Certificates with private keys protected in an HSM (SSID)
5.0	01.06.2018	Adapted to ETSI EN 319 411-1/2 and EN 319 401. Included Qualified Certificates according to eIDAS. Converted to RFC 3647 format.
5.1	20.05.2020	Adapted to new Norwegian legislation (i.e. Selvdeklarasjonsforskriften) and changed procedures for CP/CPS notifications.
6.0	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.

The Subjects are individuals registered within the National Population Register. The Subject is identified in the Certificate as the holder of the Private Key associated with the Public Key given in the Certificate.

The Subject is responsible towards Buypass CA for the use of the Private Key associated with the Certificate. The Subject must accept the terms and conditions regarding the use of the Certificate by accepting a Subject Agreement.

The entity applying for a Certificate may be different from the Subject to whom the Certificate applies. For example, the Subscriber may be an organization requiring Certificates for its employees to participate in electronic business on behalf of the organization. A Subscriber subscribes with Buypass CA on behalf of one or more Subjects by signing a Subscriber Agreement.

In other situations, a Certificate is issued directly to an individual Subject for his/her own use, i.e. the Subscriber and Subject is the same.

In some parts of this document the term Subscriber is used mainly for the case when the Subject is different from the Subscriber. In other parts of the document, the term may be used synonymously with Subject, i.e. where the Subject and Subscriber may be the same entity. In this case, the term Subject Agreement and Subscriber Agreement may also be used synonymously.

1.3.1 Certification Authorities
Buypass is the Certificate Authority (CA) for all Buypass Class 3 Qualified Certificates.

1.3.2 Registration Authorities
Buypass operates as the Registration Authority (RA) for Buypass Class 3 Qualified Certificates.

An organization applying for Certificates on behalf of it's employees may operate as a Registration Authority for these Certificates.

A Distribution Service Provider may be used to verify the identity of the Subject at time of delivery.

1.3.3 Subscribers
The Subjects are individuals registered within the National Population Register. The entity applying for a Certificate may be different from the Subject to whom the Certificate applies. For example, the Subscriber may be an organization requiring Certificates for its employees to participate in electronic business on behalf of the organization.

1.3.4 Relying Parties

1.3.5 Other Participants

1.4 Certificate Usage

1.4.1 Primary Certificate Purposes
Buypass Class 3 Qualified Certificates are applicable for supporting electronic signatures according to the Regulation (EU) No 910/2104 [19].

Buypass Class 3 Qualified Certificates may also be used to verify the identity of a person and to encrypt data and/or symmetric keys used for encryption of data.

1.4.2 Secondary Certificate Purposes

1.4.3 Excluded Certificate Purposes
Buypass Class 3 Qualified Certificates SHALL NOT be used to sign software, certificates and/or revocation lists.

Buypass Class 3 Qualified Certificates SHALL NOT 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 [17] and Certification Practice Statement[18] and their maintenance.

1.5.2 Contact Person
Contact point for questions regarding the Certificate Policy [17] and Certification Practice Statement [18] 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 [18] are 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
Advanced electronic signature	An advanced electronic signature shall meet the following requirements: • it is uniquely linked to the signatory • it is capable of identifying the signatory • it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and • it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable
Authorized Subscriber Representative	A natural person who has express authority to represent the Subscriber.
Authorized Partner Representative	A natural person who has express authority to represent the Partner.
Buypass	Buypass AS, registered in the Norwegian National Register of Business Enterprises with organization number 983 163 327.
Buypass Certification Services	CA Services as described in this Policy. Encompasses the following services: 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. Certificate generation service: creates and signs certificates based on the identity and other attributes verified by the registration service. 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. 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. Revocation status service: provides certificate revocation status information to relying parties. Subject device provision service: prepares, and provides or makes available secure cryptographic devices, or other secure devices to Subjects.
Buypass Web	Websites operated by Buypass, i.e. www.buypass.no and www.buypass.com.
Buypass Policy Board	The Board responsible for all Certificate Policies in Buypass.
Card Bureau	Entity or legal person providing a Subject device provision service, i.e. prepares the Signature Creation Device (SCDev) and/or Activation Data and distributes such objects to the Subject.

Terms	Definition
Card Issuer	Entity or legal person issuing smart cards to its customers.
Central Coordinating Register for Legal Entities (“Enhetsregisteret”)	National register containing basic data (e.g. 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 Qualified Certificate.
Certificate Applicant	Authorized Subscriber Representative who has authority to submit a Certificate application on behalf of 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.
Certificate Rekey	The issuance of a new certificate for a previously registered Subject/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 Certification Authority employs in issuing, managing, revoking or re-keying certificates (see [1]).
Contract Signer	Authorized Subscriber Representative who has authority on behalf of Subscriber to sign Subscriber Agreements.
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 Signature	Data in electronic form which are attached to or logically associated with other electronic data and which and which is used by the signatory to sign (see Regulation (EU) No 910/2014 [19]).
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.
Information Security Management System (ISMS)	A management process with a set of policies concerned with information security management and IT related risks. The best known ISMS is described in ISO/IEC 27001 and ISO/IEC 27002 and related standards published jointly by ISO and IEC.
Local Registration Authority (LRA)	An entity responsible for performing RA operations (see Registration Authority) for a limited community of Subjects. A Subscriber organization may operate as an LRA for the community of Subjects associated with the organization (i.e. the employer may act as an LRA on behalf of its employees).
Multifactor Authentication Token	A token issued by Buypass and used to authorize access to Subject’s private keys protected in an HSM. Acceptable tokens according to this document must be at an assurance levels similar to ‘eIDAS LoA substantial’ according to current national legislation.

Terms	Definition
National Identification Number	A unique 11-digit number identifying persons registered in the National Population Register. This may be an identification number assigned to persons residing permanently in Norway (“fødselsnummer”) or a temporarily identification number assigned to persons residing in Norway for a shorter period (“D-nr”).
National Population Register	Nationwide register holding National Identification Number and other information about natural persons that reside in Norway (“Freg - Folkeregister”).
Organization Number	Unique enterprise identification number as registered in the Central Coordinating Register for Legal Entities.
Partner	A legal person given the Authority to assign natural persons as Authorised Partner Representatives acting on behalf of one or more Subjects. The legal person must have signed a Contractual agreement with Buypass before acting as a Partner.
Personal Identification Number (PIN)	A code the Subject must enter to access the Private Key within a smart card, see also Activation Data.
PIN Unblocking Key (PUK)	A code used to unblock the PIN within a smart card. A PIN is blocked after 3 incorrect PIN entries. In order to unblock the PIN to get access to the Private Key the Subject must enter the PUK.
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 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.
Qualified Certificate	A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of the Regulation (EU) No 910/2014 [19].
Registration Authority (RA)	An entity that is responsible for one or more of the following functions: • the identification and authentication of Subjects and/or Subscriber representatives • the approval or rejection of certificate applications • initiating certificate revocations or suspensions under certain circumstances • processing requests to revoke or suspend certificates, and • approving or rejecting requests to renew or rekey certificates
Relying Party	Recipient of a Certificate which acts in reliance on that Certificate and/or digital signatures verified using that Certificate (see [1]).
Signature Creation Device (SCDev)	Configured software or hardware used to create an electronic signature (see Regulation (EU) No 910/2014 [19]). In this document the SCDev is either a smart card or an HSM.
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.
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.

Terms	Definition
Subject Agreement	Contractual agreement or written statement that specifies all Subject obligations under the Certificate Policy for Buypass Class 3 Qualified Certificates [17].
Subject Authentication	Verifying the identity of the Subject, i.e. verification of authentication data that prove that a particular person is in fact the Subject identified (proof-of-identity).
Subject Identification	Submission/collection of Subject identity data required to establish the unique identity of the Subject.
Subscriber	Entity subscribing with a Certification Authority on behalf of one or more Subjects. The Subject may be a subscriber acting on his own behalf.
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 Practices 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] ISO/IEC 9594-8 Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks"
[8] ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules"
[9] ISO/IEC 27002:2013: Information technology - Security techniques. Code of Practice for Information Security Management.
[10] ISO/IEC 15408 (parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security"
[11] ETSI TS 119 312 – Cryptographic Suites
[12] ETSI EN 319 401 – General policy requirements for Trust Service Providers
[13] ETSI EN 319 411-1 – Policy and security requirements for Trust Service Providers issuing certificates; Part 1 General requirements
[14] 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
[15] IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP), June 2014
[16] Buypass Class 3 Certificate and CRL profiles, current version
[17] Certificate Policy for Buypass Class 3 Qualified Certificates, current version
[18] Certification Practice Statement for Buypass Class 3 Qualified Certificates, this document
[19] 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
[20] Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften), FOR-2019-11-21-1578
[21] Lov om tiltak mot hvitvasking og terrorfinansiering mv (hvitvaskingsloven), Lov 2009-04-15
[22] FOR-2009-03-13-302 Hvitvaskingsforskriften: ”Forskrift om tiltak mot hvitvasking og terrorfinansiering mv.”
[23] CEN Workshop Agreement 14171: “General guidelines for electronic signature verification”
[24] Lov 15.juni 2018 nr 38 om behandling av personopplysninger (personopplysningsloven)

[25] Forskrift 15.juni 2018 nr 876 om behandling av personopplysninger (personopplysningsforskriften)

1.6.3 Conventions

Text that is outside text boxes is the Certificate Policy [17]. 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 Qualified Certificates.

2 Publication and repository responsibilities

2.1 Publication of information

a) The Certificate Policy for Buypass Class 3 Qualified Certificates [17] and the Certification Practice Statement for Buypass Class 3 Qualified Certificates [18] SHALL be publicly available on the Buypass web 24 hours a day 7 days per week (24x7).

The Certificate Policy for Buypass Class 3 Qualified Certificates [17] and the Certification Practice Statement for Buypass Class 3 Qualified Certificates [18] are available 24x7 and accessible on Buypass web.

b) Revocation status information SHALL be publicly available 24x7 at the location(s) specified in the appropriate extensions of every Certificate issued.

Every Buypass Class 3 Qualified Certificate contains a CRL distribution point extension that contains URLs 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 Qualified 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 Qualified 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 are published as a prerequisite when applying for a 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

The CA SHALL ensure that Subjects are properly identified and authenticated and that certificate requests are complete, accurate and duly authorized.

Only persons registered in the National Population Register are allowed to register and apply for a Certificate.

Each person in the National Population Register is identified with a National Identification Number and this must be provided together with the Subject name. The provided Subject National Identification Number and name are verified online towards the National Population Register at initial registration time.

The Subject name and address as registered in the National Population Register are stored and kept for subsequent use in Buypass' register of Subjects. This Subject information is kept up to date with the National Population Register.

3.2.1 Method to Prove Possession of Private Key

The CA SHALL warrant that the Subject named in a Certificate is in possession of the Private Key that corresponds to the Public Key in that Certificate.

The Private Key associated with the Public Key in a Buypass Class 3 Qualified Certificate is always protected within a Signature Creation Device (SCDev), this is either a smart card or an HSM.

For Private Keys protected in a smart card, Buypass supports two schemes for key generation:

Scheme 1:
Central generation of the Subject's key pair performed under Buypass' control within the CA operations facilities. The Private Key is generated within an HSM and thereafter securely loaded into the smart card.

Scheme 2:
Local generation of the Subject's key pair performed under Subject's control. The Private Key is generated in the smart card. The local key generation may be either

a) guided by an Authorized Subscriber Representative or

b) performed by the Subject himself/herself.

Buypass guarantees that the Subject named in the Certificate is in possession of the Private Key that corresponds to the Public Key in the Certificate as follows:

Scheme 1:
For the central key generation, the Subject's key pair and corresponding Certificate generation is performed

before the smart card is distributed to the Subject. The possession guarantee is based on a controlled preparation and distribution of the smart card and associated Activation Data. The verification of Subject identity is done according to 3.2.3.2 at time of delivery.

Scheme 2:
For the local key generation, the Subject's key pair is generated in the smart card and under Subject control.

a) If the process is guided by an Authorized Subscriber Representative, the possession guarantee is based on a verification of Subject identity at time of issuance. The Subscriber is responsible for verifying the identity of the Subject according to this document.

b) If the process is performed by the Subject himself/herself, the possession guarantee is based on an on-line verification of Subject identity. Such an on-line verification may be by

c) means of presenting Activation Data distributed to the Subject requiring physical presence and

d) verification of Subject identity according to 3.2.3.2.

For Private Keys protected in an HSM, the Subject's key pair is generated within the HSM and protected cryptographically such that they are unavailable for use until being assigned to the Subject defined in the Certificate. The HSM is controlled by Buypass within the CA operations facilities.

The Subject must use a Multifactor Authentication Token under Subject control to authorize the access to the Private Key. A Multifactor Authentication Token is issued by Buypass and cryptographically connected to the Private Key such that the Private Key is only accessible by using this token, i.e. the Private Key is under Subject sole control.

The possession guarantee is based on verification of Subject identity according to 3.2.3.2 before the Private Key is accessible. This may be done by distribution of Activation Data to the Subject requiring physical presence. Such Activation Data may be explicit for the activating the Private Key or implicit for activating the Multifactor Authentication Token.

a) If the CA generates the Subject's key:
   - the procedure of issuing the Certificate SHALL be securely linked to the generation of the key pair by the CA
   - the Private Key SHALL be securely made available to the registered Subject

For Private Keys protected in a smart card, key generation and Certificate issuance are performed in one operation, see 4.3.1 a). Regarding secure distribution of the Private Key, see 3.2.1 and 6.1.2.

For Private Keys protected in an HSM, key generation may be performed earlier than the issuance of the Certificate. The Private Key is unavailable for use until assigned to the Subject defined in the Certificate. Regarding how to access the Private Key, see 3.2.1 and 6.2.8.

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

The Private Key may be generated within the smart card under Subject/Subscriber control.

However, Buypass controls the key generation and subsequent certificate issuance using a trusted channel. This ensures that the Subject/Subscriber in possession of the smart card also possesses the Private Key. See 3.2.1 and 4.3.1 a)

3.2.2 Authentication of Organization Identity

This section is relevant only when the Subscriber is different from the Subject.

The following Subscriber information SHALL be obtained prior to any Subject initial registration:

- full name and legal status of the Subscriber as defined in the Central Coordinating Register for Legal Entities
- the Subscriber's Organization Number as defined in the Central Coordinating Register for Legal Entities
- name and contact information of Subscriber Representatives authorized to operate as Contract Signer or Certificate Manager

As part of an initial Subscriber Registration and Subscriber Agreement Signing the Subscriber will register the following information with Buypass:

- the Subscriber's Organization Number and name as registered in the Central Coordinating Register for Legal Entities
- the Contract Signer's name and contact information
- the Certificate Manager's name, National Identification Number and contact information

The Subscriber's Organization Number and name and its legal status are verified against the Central Coordinating Register for Legal Entities. If the verification fails, the Subscriber registration is rejected.

The Certificate Manager's name and National Identification Number are verified against the National Population Register. If the verification fails, the registration of the Certification Manager is rejected.

All information is incorporated into a Subscriber Agreement that is signed by the Contract Signer.

3.2.3 Authentication of Individual Identity

3.2.3.1 Identification of Subject

a) The CA SHALL warrant that a Buypass Class 3 Qualified Certificate is linked to one (1) unique natural person registered in National Population Register.

During the registration process the provided Subject name and National Identification Number are verified against the National Population Register. This initial registration is performed either prior to, or at the time of the Certificate application.

The provided Subject name and National Identification Number must match the corresponding information in the National Population Register according to defined matching rules.

If the Subject does not exist in the National Population Register, the registration is rejected.

b) The CA SHALL ensure over time the uniqueness of the distinguished name assigned to the Subject within the domain of the CA, i.e. over the life time of the CA a distinguished name which has been used in an issued Certificate SHALL never be re-assigned to another entity.

Buypass assigns a unique identification number to the Subject at time of registration.

This identification number is included as a part of the Subject Serial Number in the Subject Distinguished Name (DN) of a Certificate and ensures the uniqueness of the Subject DN.

3.2.3.2 Authentication of Subject

The CA SHALL verify the identity of the person to which a Buypass Class 3 Qualified Certificate is issued. The verification SHALL either be checked against the physical person directly or indirectly using means providing equivalent assurance as physical presence.

The verification of Subject identity at initial registration is according to relevant parts of "Hvitvaskingsforskriften" [22] and the verification may be performed either by:

- a Distribution Service Provider before delivery of the smart card and/or Activation Data to the Subject
- an Authorized Subscriber Representative at the time of Certificate application
- an authorized representative for a third party as defined in "Hvitvaskingsloven" [21]

- Buypass

The Subject identity is verified against a natural person presenting a valid identity document as defined in "Selvdeklarasjonsforskriften" [20].

Procedures exist to verify that the identity document is valid and to ensure that the identity of the Subject is properly verified.

The initial registration may be performed as an integrated process related to the issuance of a Multifactor Authentication Token (e.g. smart cards without Certificates). Such authentication tokens must be used to generate Activation Data authorizing access to Private Keys protected in an HSM.

Authentication tokens like smart cards may also be updated with Certificates later using a post-issuance Certificate application service.

The initial registration may be performed prior to Certificate application and the subsequent Certificate application may be based on this initial authentication of the Subject.

3.2.3.3 Identification and authorization of Subscriber representatives

This section is relevant only when the Subscriber is different from the Subject.

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

The Subscriber may authorize a single person to fill one, two or all three of these roles. The Subscriber may authorize more than one person to fill each of these roles. An authorized Certificate Manager is by definition also an authorized Certificate Applicant.

A Certificate Manager registers the Certificate Applicant's name, National Identification Number and contact information with Buypass.

The Certificate Applicant's name and National Identification Number are verified against the National Population Register. If the verification fails, the registration of the Certificate Applicant is rejected.

3.2.3.4 Authentication of Authorised Subscriber Representatives

This section is relevant only when the Subscriber is different from the Subject.

Before a new Certificate is issued to a Subject the Authorised Subscriber Representative (Certificate Manager or Certificate Applicant) SHALL be authenticated.

The Authorized Subscriber Representative authenticates himself/herself electronically using a valid Certificate.

3.2.4 Non-verified Subscriber Information

3.2.5 Validation of Authority

a) A Contract Signer's Signing Authority SHALL be established through a Signing Authority Statement. Accepted Signing Authority Statements MAY be:
   - information obtained from the Central Coordinating Register for Legal Entities 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 the Central Coordinating Register for Legal Entities

Buypass initially consults the Central Coordinating Register for Legal Entities directly to verify whether the identified Contract Signer has a defined role in the Central Coordinating Register for Legal Entities.

If this verification step fails Buypass contacts the Subscriber with instructions to obtain a Signing Authority Statement. Buypass verifies the authenticity of such a Signing Authority Statement by contacting the person who has issued it.

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.

b) A Certificate Manager's 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.

c) A Certificate Applicant's authority SHALL be established through
- an express authorization statement issued by an authorized Contract Signer or Certificate Manager

The Certificate Manager may explicitly authorize one or several Certificate Applicants to submit Certificate applications on behalf of the Subscriber.

3.2.6 Criteria for Interoperation or Certification

3.3 Identification and authentication for re-key requests

The CA SHALL ensure that requests for certificates issued to a Subject who has already previously been registered are complete, accurate and duly authorized. This includes rekey following revocation or prior to expiration.

3.3.1 Identification of Subject

The CA SHALL warrant that a Buypass Class 3 Qualified Certificate is linked to one (1) unique natural person registered in the National Population Register.

Certificate Rekey is based on previously registered Subject data.

The Subject National Identification Number, name and address as registered in National Population Register are stored and kept for subsequent use in Buypass' register of Subjects. The Subject information is kept up to date with the National Population Register.

Alternatively, the Subject National Identification Number and name must be provided at time of Certificate Rekey. The provided Subject National Identification Number and name must match the corresponding registered Subject data according to defined name matching rules.

3.3.2 Authentication of Subject

The CA SHALL ensure that Subjects are properly identified and authenticated and that certificate requests are complete, accurate and duly authorized.

The Certificate Rekey may be requested by

1) the Subject himself/herself
2) a Partner on behalf of the Subject
3) Buypass
4) an Authorized Subscriber Representative acting on behalf of the Subject, i.e. when the Subscriber is another entity than the Subject

If the Subject requests a Certificate Rekey, the Subject may be authenticated by:

a) using a valid Certificate

b) using other electronic identification providing equivalent assurance to physical presence

c) implicit authentication by distributing the Certificate to Subjects address according to the National Population Register

d) the Distribution Service Provider before delivery of a smart card and/or Activation Data

A Partner may request a Certificate Rekey on behalf of the Subject. The Authorized Partner Representative is authenticated by using a valid Certificate. The Subject may be authenticated by

a) implicit authentication by distributing the Certificate to Subject's address according to the National Population Register

b) the Distribution Service Provider before delivery of the smart card and/or Activation Data

Buypass may request a Certificate Rekey. The Subject may be authenticated by

a) implicit authentication by distributing the Certificate to Subjects address according to the National Population Register

b) the Distribution Service Provider before delivery of the smart card and/or Activation Data

If the Certificate Rekey is requested by an Authorized Subscriber Representative, the authentication of the Subject will be performed either by using a valid Certificate or by the Authorized Subscriber Representative where the Subject will be authenticated by:

a) presenting a valid identity document as defined in "Selvdeklarasjonsforskriften" [20]

b) a control against a recorded copy of an identity document used on a previous occasion in combination with a third person's confirmation of the Subject identity

3.3.3 Identification and authentication of Subscriber and Subscriber representatives

In case the Subscriber is different from the Subject, the requirements for identification and authentication of Subscriber and Authorized Subscriber Representatives are the same as for initial registration (see 3.2.2, 3.2.3.3 and 3.2.3.4).

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

If the Subscriber needs to make changes to any of the registered information and/or authorizations before a routine rekey, the statements in 3.2.2, 3.2.3.3 and 3.2.3.4 applies.

3.3.4 Proof of possession of Private Key

The proof of possession of the Private Key for Certificate Rekey application is similar to Initial Registration, see chapter 3.2.1.

The proof of possession of the Private Key, either protected in a smart card or in an HSM may be done as for initial application, see 3.1.6.

The possession proof for a rekey application may also be based on a proper authentication of Subject at time of certificate application, e.g. by using a valid certificate or other electronic means providing similar assurance as physical presence.

3.4 Identification and authentication for revocation request

a) Only the Subscriber or an Authorized Subscriber Representative MAY request Certificate revocation on behalf of the Subscriber.

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

If the Subscriber or none of the already Authorized Subscriber Representatives can be contacted, Buypass will authorize the Revocation Request only if the originator of the request can be identified as a new Authorized Subscriber Representative.

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

See 4.4.3 b)

4 Certificate life-cycle operational requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 Initial application submitted by Subject

a) The Subject SHALL register with an RA either prior to, or at the time of, applying for a Certificate. 3.2 defines necessary requirements for identification and authentication.

The application procedure consists of the following steps:

1. Subject enrollment: The Subject registers Subject information as defined in 3.1.1.
2. Request for Certificate issuance: The Subject applies for a Certificate according to operational requirements defined in this section.

Step 1) and 2) may be performed in one operation.

The Subject may explicitly authorize a Partner to submit the Certificate application on behalf of the Subject. I.e. the Authorized Partner Representative may perform the Subject enrollment and/or request for Certificate Issuance on behalf of the Subject.

The request for Certificate issuance may be:

1. included in a request for a smart card comprising Certificates or
2. a request for Certificates in a smart card already in the possession of the Subject
3. a request for Certificates for private keys protected in an HSM

In case 1) the central key generation scheme (scheme 1) is used and the personalized smart card and corresponding Activation Data will be securely delivered to the Subject.

In case 2) the local key generation scheme (scheme 2) is used and the key pair is generated in the smart card under Subject control. Buypass distinguish between two situations:

a) The smart card is locked for further use at time of issuance and protected with a randomly generated Activation Data. This Activation Data is securely delivered to the Subject using a Distribution Service Provider.

b) The certificates are activated at time of issuance provided that the Subject is authenticated by electronic identification using means providing equivalent assurance to physical presence.

In case 3) the Private Key is generated in an HSM and the access to the Private Key is locked until the Subject is properly authenticated by using a Multifactor Authentication Token authorizing access to the Private Key is cryptographically connected to the Private Key.

b) The Subject SHALL accept the terms and conditions regarding the use of Buypass Class 3 Qualified Certificates including consent to the keeping of a record by the CA of information used in the registration.

Terms and conditions are made available to the Subject through a Subject Agreement.

The Subject Agreement is made available to the Subject electronically during the Certificate application and/or on written paper distributed with the smart card or Activation Data.

The Subject must accept the terms and conditions regarding the use of the Certificates in order to complete the Certificate application.

If the Subject has authorized a Partner to submit the Certificate application, the Subject has accepted the terms and condition at time of authorizing the Partner.

4.1.1.2 Initial application submitted by Subscriber representative

The Subscriber SHALL register prior to applying for a Certificate on behalf of a Subject. 3.2 defines necessary requirements for identification and authentication.

a) The Contract Signer, Certificate Manager and Certificate Applicant SHALL register prior to applying for a Certificate on behalf of a Subject associated with the Subscriber.

The Subscriber is a legal person with which the Subject is associated (e.g. employed).

The application procedure consists of the following steps:

1. Subscriber Registration and Subscriber Agreement Signing: The Subscriber registers Subscriber information as defined in 3.2 as well as proof of authorization for Contract Signers and Certificate Managers as described in 3.2.3.3. The Subscriber also provides a Subscriber Agreement signed by the authorized Contract Signer.
2. Subject enrollment: A Certificate Manager identified and authorized as part of Subscriber Registration (see 3.2.3.3) registers with Buypass Subject information as defined in 3.2.3.1.
3. Request for Certificate issuance: A Certificate Manager or Certificate Applicant identified and authorized as described in 3.2.3.3 provides to Buypass a request for Certificate issuance.

The request for Certificate issuance may be:

1. included in a request for a smart card comprising Certificates or
2. a request for Certificates in a smart card already in the possession of the Subject
3. a request for Certificates protected in an HSM

In case 1) the central key generation scheme (scheme 1) is used and a personalized smart card and corresponding Activation Data will be delivered to the Subject by a Distribution Service Provider. The Distribution Service Provider will verify the identity of the Subject according to 3.2.3.2.

In case 2) the local key generation scheme (scheme 2) is used and the key pair is generated in the smart card under Subject and Subscriber control. The Authorized Subscriber Representative requesting the Certificate will verify the identity of the Subject according to 3.2.3.2.

In case 3) the key is generated in the HSM under Subject and Subscriber control. The Authorized Subscriber Representative requesting the Certificate will verify the identity of the Subject according to 3.2.3.2 before Subject is granted access to the Private Key using a Multifactor Authentication Token.

b) The CA SHALL inform the Subscriber of the terms and conditions regarding the use of Buypass Class 3 Qualified Certificates before Certificate activation.

The Subscriber Agreement refers to the Certificate Policy for Buypass Class 3 Qualified Certificates [17] which includes all relevant terms and conditions.

c) The Subject SHALL accept the terms and conditions regarding the use of Buypass Class 3 Qualified Certificates including consent to the keeping of a record by the CA of information used in the registration.

All relevant terms and conditions regarding use of Certificates are made available to the Subject through a Subject agreement which the Subject must give his/her explicit consent to.

The Subject agreement also includes a statement regarding the keeping of information used in the registration.

4.1.2 Enrollment Process and Responsibilities

a) The CA SHALL ensure that certificate requests are complete, accurate and duly authorized.

A Certificate application may be submitted by the Subject himself/herself.

The Subject may explicitly authorize a Partner to submit the Certificate application on behalf of the Subject.

In case the Subscriber is different from the Subject, a Certificate application may be submitted from an Authorized Subscriber Representative.

Certificate applications are submitted electronically by web-based services and/or applications provided by Buypass.

b) The confidentiality and integrity of application data SHALL be protected, especially when exchanged between the Subscriber, Subject or between distributed RA and CA system components.

Buypass offers TLS-protected web-based RA services. The SSL certificate identifies Buypass as the domain owner.

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

A Subscriber may operate as a Local Registration Authority (LRA) and an Authorized Subscriber Representative may apply for Certificates as defined in 4.1.1.2. The Authorized Subscriber Representative authenticates himself/herself using a valid Certificate.

4.2 Certificate application processing

4.2.1 Performing Identification and Authentication Functions

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 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.

4.2.2 Approval or Rejection of Certificate Applications

4.2.3 Time to Process Certificate Applications

4.3 Certificate issuance

4.3.1 CA Actions during Certificate Issuance

a) 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.

Buypass supports two different schemes for Subject key generation for Private Keys protected in a smart card:

Scheme 1:
Central generation of the Subject's key pair performed under Buypass control within the CA operations facilities. The Private Key is generated in an HSM and thereafter securely loaded onto the smart card.

Scheme 2:
Local generation of the Subject's key pair performed under Subject control. The Private Key is generated in the smart card. Buypass establishes a trusted channel between the smart card and a physically secured environment within the CA operation facilities. This channel is used to trigger the key generation within the smart card and also to exchange the Public Key and the Certificate between the smart card and the CA. The Private Key is under Subject sole control.

Key generation and Certificate issuance are performed as one operation for both schemes, i.e. Buypass authorizes the key generation and subsequent certificate issuance, even though the smart card is under Subject control in scheme 2.

For Private Keys protected in an HSM, the Subject's key pair is generated within the HSM and protected cryptographically such that they are unavailable for use until being assigned to the Subject defined in the Certificate. The HSM is controlled by Buypass within the CA operations facilities.

The Private Key may be generated initially and kept encrypted and unavailable for use until it is assigned to the Subject at a later stage.

The Subject must use a Multifactor Authentication Token under Subject control to authorize the access to the Private Key. A Multifactor Authentication Token is issued by Buypass and cryptographically connected to the Private Key such that the Private Key is only accessible by using this token, i.e. the Private Key is under Subject sole control.

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

The Certificate application data is stored and managed by a trustworthy system protecting the data and ensuring the integrity of such data.

The Certificate issuance is based on these registered Certificate application data ensuring that key pairs and Certificates are generated, linked and distributed to the correct Subject.

4.3.2 Notification of Certificate Issuance

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The CA SHALL ensure that the Subject/Subscriber confirms that the information held in the certificate is correct.

The Subject/Subscriber must confirm that any Subject data to be included in the Certificate is correct at the time of Certificate application.

If the Subject has authorized a Partner to submit the Certificate application, the Partner must confirm that the information is correct on behalf of the Subject.

The integrity protection of Certificate application data (see 4.3.1) ensures that the Subject data to be included in the Certificate is correct.

4.4.2 Publication of the certificate by the CA

a) The CA SHALL ensure that the Certificates are made available as necessary to Subscribers, Subjects and Relying parties.

For Private Keys protected in a smart card, the corresponding Certificate is delivered to the Subject in the smartcard.

For Private Keys protected in an HSM, the Certificates are available for the Subject through an online service.

Certificates are made publicly available to Relying Parties through a directory service, see 2.1.

b) The CA SHALL make available to Relaying Parties the terms and conditions regarding the use of Buypass Class 3 Qualified Certificates.

The terms and conditions are made available to Relying Parties on Buypass Web.

4.4.3 Notification of certificate issuance by the CA to other entities

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

4.6.1 Circumstance for certificate renewal

4.6.2 Who may request renewal

4.6.3 Processing certificate renewal requests

4.6.3.1 Rekey application submitted by Subject

The requirements in 4.1.1.1 SHALL apply also to a rekey application, whether the Certificate application involves a routine rekey or a rekey after revocation.

Buypass provides web-based administration services where Certificates are used. Subjects using these services are notified that the Certificate is about to expire two months before the expiry date.

Buypass or the Card Issuer notifies the Subject by e-mail two months prior to the Certificates expiry date.

In the case that Subject has explicitly authorized a Partner to perform the initial Certificate application, the Partner is responsible for notifying the Subject and an Authorized Partner Representative will submit the rekey application.

The Subject handles rekey application using a similar procedure as for the initial application, see 4.1.1.1. However, Subject enrollment is omitted and the Certificate application is based on registered Subject data stored in Buypass' register of Subjects. The Subject information is kept up to date with the National Population Register.

The Subject may contact Buypass or the Card Issuer by phone, e-mail or on Buypass web for the rekey application.

The requirements regarding Subject authentication are as defined in 3.3.2 for rekey application.

4.6.3.2 Rekey application submitted by Subscriber representative

The requirements in 4.1.1.2 SHALL apply also to a rekey application, whether the Certificate application involves a routine rekey or a rekey after revocation.

The Subscriber notifies the Subject when a Certificate is about to expire.

The Subscriber handles rekey using similar procedures as for the initial application, see 4.1.1.2. Subject enrollment is omitted and the Certificate application is based on previously registered Subject data which is updated with information in the National Population Register.

The requirements regarding Subject authentication are as defined in 3.3.2 for rekey application.

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

See 4.6

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 Subjects can submit revocation requests either by phone, e-mail or the Buypass web.

Authorized Subscriber Representatives may in addition submit revocation requests or revoke Certificates using web-based services and/or applications provided by Buypass.

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 Subject or 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 or 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 endeavors to ensure that this information service is not unavailable 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 is 99,8% and any loss of availability will not last more than 4 hours at a time.

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) 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 Subject/Subscriber requests revocation of its Certificate
- the Subject/Subscriber indicates notifies the CA that the original Certificate Application was not authorized and does not retroactively grant authorization
- the CA obtains evidence that the Subject'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 that a Subject has violated one or more of its material obligations under the Subject 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 [17] or the Certification Practice Statement [18]
- 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. that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced within a given period of time)
- the Subject/Subscriber does not pay the service fees to Buypass (see 9.1)
- the Subscriber ceases to exist
- the Subject is registered dead in the National Population Register

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 [17] or Certification Practice Statement [18].
- 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. that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced within a given period of time)

4.9.2 Who Can Request Revocation

a) Only the Subscriber or an Authorized Subscriber Representative-MAY request Certificate revocation on behalf of the Subscriber.

Certificate revocation may be requested by the Subscriber or an Authorized Subscriber Representative.

Buypass accepts revocation requests from unregistered Subscriber representatives only if

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

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

b) The CA or RA MAY revoke a Certificate if the CA/RA has reason to believe that a valid revocation reason exists.

Buypass is entitled to, and will revoke a Certificate, at any time for any of the reasons set forth in 4.9.1.

c) A revocation request received from a non-authorized requestor SHALL be investigated by the RA and the Subject and/or Subscriber SHALL be consulted if necessary.

If a revocation request is received and Buypass is not able to establish the requestor neither as the Subject nor an Authorized Subscriber Representative, Buypass will contact the Subject or 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.

4.9.3 Procedure for Revocation Request

a) Subject or Subscriber 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 Subject and Subscriber.

Buypass offers a 24x7 revocation service where Subjects and Authorized Subscriber Representatives may submit revocation requests by phone, e-mail or the Buypass web. Contact points for revocation are communicated to the Subject through the Subject Agreement and the Subscriber through the Subscriber Agreement. The contact points are also available on the Buypass web.

For Subscribers operating as a Local Registration Authority (LRA), the Authorized Subscriber Representatives may submit revocation requests electronically directly to the CA.

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.

4.9.4 Revocation Request Grace Period

a) For revocation reasons other than key compromise, the Subject or 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 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 either 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 on-line revocation status service.

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

b) The OCSP service SHALL be updated at least every 24 hours, and OCSP responses from this service SHALL have a maximum expiration time of 48 hours.

The OCSP service has direct access to the master source of revocation information and is therefore immediately updated whenever a Certificate is either revoked or suspended.

c) 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.

d) 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 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

If an RA is not able to process a Certificate revocation request, the Certificate SHALL be suspended until the revocation request has been properly processed.

A Certificate MAY be suspended if:

- a revocation request cannot be confirmed by an authorized source in due time
- there is reason to believe that there exist a valid revocation reason (see 4.9.2 c)), but this is not yet confirmed

If a Certificate has been suspended, 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 not be kept suspended for longer than is necessary.

If a Certificate is suspended due to lack of confirmation from an authorized source in due time, the Certificate is either revoked or unsuspended as soon as the original revocation request is confirmed or rejected by an authorized source.

If a Certificate is suspended on the basis of a suspected revocation reason, the Certificate will be either revoked or unsuspended as soon as the revocation reason has been confirmed or rejected.

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 [9] 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 [12], ETSI EN 319 411-1 [13] and ETSI EN 319 411-2 [14];

c) Protect the confidentiality, integrity, and availability of: (i) all certificate requests and data related thereto (whether obtained from Subscriber 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.

Buypass' ISMS includes regular risk assessments that:

a) Identify internal and external risks that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Data or Processes;

b) Assess the likelihood and potential damage of these risks, taking into consideration the sensitivity of the Data and Processes; and

c) Consider the effectiveness of the policies and guidelines, procedures, information systems, technology, and other arrangements that the CA has in place to control such risks.

Based on such Risk Assessment, the CA develops, implements, and maintains security procedures, measures, and products designed to achieve the objectives set forth above and 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, subject device provision and revocation management services SHALL be limited to properly authorized individuals.

Access to Buypass' CA facilities is 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 facilities is protected with several tiers of 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 of 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 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 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.

The Security Manager 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.

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 organized 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

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 Security Manager.

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 [17] 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 [18] 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 [17] and the Certification Practice Statement [18]. 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 9.6.2 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 a 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.

b) All events related to registration including requests for certificate re-key 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. subject'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. method used to validate identification documents, if any; and
   v. 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 4.1.1.1 b)

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

See 9.3

g) The record requirements in 5.4.1 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 and revocation requests
   - all verification activities required
   - acceptance and rejection of Certificate applications
   - issuance of Certificates
   - suspension and revocation of Certificates
3. Subject key lifecycle management events, including
   - Key generation
4. Requests and reports relation to revocation
   - generation of Certificate Revocation Lists (CRLs)
   - OCSP entries
5. security events, including:
   - changes related 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 and 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.

All logging is carried out in compliance with Norwegian laws and relevant EU regulations (e.g. [19])

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

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

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 only authorized persons have had access. Other logs are processed as needed. Real-time alerts are in place for important events.

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 4.5.2 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.

Segregation of duties is used to ensure that only a limited number of persons in trusted roles have access to the audit records.

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. Also see 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 9.6.2 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 in compliance with Norwegian laws 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 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 Subjects, 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 Subjects, 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 Subjects, 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 all Certificates, if required

The Buypass CA termination plan includes all requirements above.

c) The CA SHALL have an arrangement to cover the costs to fulfill 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 fulfillment 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 [8] or FIPS PUB 140-2 [5] level 3 or higher
- is a trustworthy system which is assured to EAL 4 or higher according to ISO/IEC 15408 [10] or or equivalent 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 generated in an HSM compliant to FIPS 140-2 level 3 [5].

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

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

For Private Keys protected in a smart card Buypass supports two different schemes for Subject key generation.

Scheme 1:
Central generation of the Subject's key pair performed under Buypass control. In this case the Private Key is generated in an HSM and thereafter securely loaded onto the smart card. The secure loading of the Private Key may be performed at Buypass premises or at a Card Bureau. The Private Key is in this case generated within an HSM compliant to FIPS 140-2 level 3 [5].

Scheme 2:
Local generation of the Subject's key pair performed under Subject control. In this case the Private Key is generated in the smart card. Buypass establishes a trusted channel between the smart card and a physically secured environment within the CA operations facilities. This channel is used to trigger the key generation

process within the smart card and also to exchange the Public Key and the Certificate between the smart card and the CA.

For Private Keys protected in an HSM Buypass generates the key pair in the HSM and the Private Key is protected cryptographically such that it is unavailable for use until being assigned to the Subject.

b) CA generated Subject keys SHALL be generated and stored securely before being made available for the Subject.

For Private Keys protected in a smart card and the key pairs are generated centrally, the Private Keys are cryptographically protected with a cryptographic strength equivalent to at least 112 bits symmetric key until loaded onto the smart card.

For Private Keys protected in an HSM, the Private Keys are cryptographically protected with a cryptographic strength equivalent to at least 256 bits symmetric key until being assigned to the Subject.

6.1.2 Private Key Delivery to Subscriber

a) The Subject Private Key SHALL be made available to the Subject in a manner such that the secrecy and integrity of the key is not compromised and, once made available to the Subject, the Private Key can be maintained under the Subject's sole control. 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 Private Keys protected in a smart card, the Private Keys are delivered to the Subject according to two different key generation schemes:

Scheme 1:
With central key pair generation, the Private Key is securely loaded on the smart card and distributed to the Subject.

Scheme 2:
With local key pair generation, the Subject's key pair is generated in the smart card under Subject or Subscriber control.

Verification of Subject identity is performed according to 3 ensuring that the Private Key is under Subject sole control. The Subject maintains sole control of the Private Key in the smart card by means of physical access to the smart card and a personal PIN.

For Private Keys protected in an HSM, the Private Keys are accessible by the Subject only by electronic means based on a Multifactor Authentication Token. This token is issued by Buypass and cryptographically connected to the Private Key such that access to the Private Key is available only for connected tokens controlled by Subject. I.e. the Private Key is under Subject's sole control.

The Subject may use several tokens to authorize access to the same Private Key protected in an HSM. Each token is issued to the Subject and connected individually to the Private Key.

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

For Private Keys protected in a smart card and the key pairs are generated centrally (i.e. scheme 1), routines are in place to ensure that copies of the Subject Private Key are destroyed within reasonable time after the key is delivered to the Subject. This is valid both for Buypass and the Card Bureau.

For Private Keys protected in an HSM, the Private Keys are always under Subject's sole control by cryptographic means and no copies of the Private Key exist.

6.1.3 Public Key Delivery to Certificate Issuer

If the Subject's key pair is not generated by the CA, the certificate request process SHALL ensure that the Subject has possession of the Private Key associated with the Public Key presented for certification.

With local key pair generation (i.e. Scheme 2), the Subject's key pair is generated in the smart card and under Subject control.

1. If the process is supervised by an Authorized Subscriber Representative, the possession proof is based on a verification of Subject identity at time of issuance. The Subscriber is responsible for verifying the identity of the Subject according to this document.
2. If the process is performed by the Subject himself/herself, the possession guarantee is based on an on-line verification of Subject identity. Such on-line verification may be

a) based on a previously issued electronic identity requiring physical presence similar to the requirements in this document or

b) by means of presenting Activation Data distributed to the Subject requiring physical presence and verification of Subject identity at time of delivery.

In these cases the Private Key is generated in the smart card. Buypass establishes a trusted channel between the smart card and a physically secured environment in the CA facilities. This channel is used to trigger the key generation and also to exchange the Public Key and the Certificate between the smart card and the CA. The Private Key is under Subject's sole control.

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

The issuing CA and Root CA Certificates may also be downloaded from the 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 [7]

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

CA keys

a) CA key pair generation SHOULD be performed using an algorithm as specified in ETSI TS 119 312 [11] 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 [11] 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 CA Root CA key is RSA 4096 bits. Root CA signatures on CA Certificates and CRLs for CA Certificates are based on this key and using SHA-256 as hash algorithm.

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

Subject keys

c) Subject keys SHALL be generated using an algorithm which are recognized by industry as being fit for the uses identified in this Certificate Policy during the validity time of the Certificate, see [11].

d) Subject keys SHOULD be of a key length and for use with a public key algorithm as specified in ETSI TS 119 312 [11] for the purposes stated in this Certificate Policy during the validity time of the certificate.

Only RSA Subject keys are supported, the key size are at least 2032 bits for private keys protected in a smart card and 2048 bits for private keys protected in an HSM.

6.1.6 Public Key Parameters Generation and Quality Checking

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 Buypass Class 3 Certificate and CRL profiles [16] and compliant with the SEID profile for certificates issued to natural persons [6].

Certificates are used for Private Keys protected in Signature Creation Devices (SCDev) and they are always comprised of 2 different key pairs. One key pair is used for authentication and encryption and the other is used for electronic signature only.

The key usage combinations for Certificates are described in Buypass Class 3 Certificate and CRL profiles [16].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CA keys

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 b)

The Buypass Class 3 CA Private Keys are protected by and used within an HSM compliant to FIPS 140-2 level 3 [5].

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.

All signing operations that involve the CA Private Key are performed in Buypass' CA operations facility (see 5.1.1).

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 HSM. 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.

Subject keys
The following requirements apply to the cryptographic module hosting the Subject keys protected in an HSM;

h) The Subject key SHALL be held and used within a secure cryptographic module which meets the requirements identified in ISO/IEC 19790 [8] or FIPS PUB 140-2 [5] level 3.

The Subject Private Keys are protected by and used within an HSM compliant to FIPS 140-2 level 3 [5].

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

The Subject Private Keys are encrypted and connected cryptographically to a Multifactor Authentication Token under Subject's sole control.

j) Where the Subject Private 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 Subject Private Keys are stored and protected by an HSM where access control mechanisms ensure that the Private Key is not accessible outside the module.

k) Operations using the Subject Private Key SHALL only take place in a physically secured environment.

All operations that involve the Subject Private Key are performed in Buypass' CA operations facility (see 5.1.1).

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 does 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. The CA Private Key is only accessible for use within an HSM and access to the key must be authorized by using a smart card.

Subject Private Key

b) Subject Private Keys SHALL be activated by means of Activation Data.

For Private Keys protected in a smart card, the access to the Private Key is protected by a PIN.

In some cases, the access to the Private Key is locked until the Subject has presented one time only Activation Data. This method may be used in the local key generation scheme (scheme 2) where the Subject requests a Certificate himself/herself. Such Activation Data is delivered securely to the Subject.

For Private Keys protected in an HSM, the Private Keys are accessible by the Subject by using a Multifactor Authentication Token under Subject control. This token is issued by Buypass and cryptographically connected to the Private Key such that access to the Private Key is available only for connected tokens controlled by Subject. I.e. the Private Key is under Subject's sole control.

The Subject may use several authentication tokens to authorize access to the same Private Key protected in an HSM. Each token is issued to the Subject and connected individually to the Private Key.

6.2.9 Deactivating Private Keys

Every time the Subject Private Key is to be used, the Subject has to provide the Activation Data, i.e. the Private Key is automatically deactivated.

For Private Keys protected in a smart card, the Subject must authorize access to the Private Key using the PIN for each operation.

For Private Keys protected in an HSM, the Subject must authorize access to the Private Key using a Multifactor Authentication Token cryptographically connected to the Private Key. Each operation involving the Private Key requires a new authorization from Subject.

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).

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 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.

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

Subject's key pairs have a total lifetime of up to 5 years, the same lifetime as the corresponding Certificate.

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

e) The Subject Public Keys may be used for verification purposes 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 not be easy to guess.

The Subject Private Keys within a smart card are protected by a PIN code which is at least 4 digits. The initial PIN code generation and installation depends on the key generation scheme used:

1. For central key generation, the initial PIN code is generated randomly by Buypass and distributed to the Subject. The Subject may set a new PIN code on receipt of the initial PIN code.
2. For local key generation; the initial PIN code is provided by the Subject.

If the local key generation process is supervised by an Authorized Subscriber Representative, the Subject sets the PIN as a part of the issuance process.

For Private Keys protected in an HSM, the Activation Data is represented by a Multifactor Authentication Token under Subject's sole control.

The Subject may use several authentication tokens to authorize access to the same Private Key protected in an HSM. Each token is issued to the Subject and connected cryptographically and individually to the Private Key.

Each token is individually connected to the Private Key after verifying that the token satisfies the requirements for being used as Activation Data for the Private Key according to this document. Only multifactor tokens issued by Buypass satisfying these requirements are allowed to be used as Activation Data. The requirements are token specific and based on a risk assessment.

6.4.2 Activation data protection

a) The CA Private Key Activation Data SHALL be protected in a physically secured environment under dual control.

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.

For Private Keys protected in a smart card, the Subject Private Key Activation Data (i.e. the PIN code) is kept inside the smart card and verified in the smart card 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 smart card is locked.

In order to unlock the PIN, the Subject may present a PIN Unlocking Key (PUK). The PUK is distributed to the Subject by a Distribution Service Provider and is under the Subject's sole control. The PUK consists of 8 digits.

The unlocking operation may be handled by an Authorized Subscriber Representative. In this case the PIN may be unlocked using a PIN unlocking code distributed electronically from Buypass' central systems through a trusted channel – see 6.1.1. This operation requires the Subject to present a valid identity document – see 3.3.2.

When the PIN is unlocked, the PIN retry counter is reset to 3.

For Private Keys protected in an HSM, the Activation Data is represented by a Multifactor Authentication Token under Subject's sole control.

The token is used to authorize access to the Private Key by means of a successful authentication combined with an authorization for using the Private Key for each individual operation. Any unsuccessful authentication and/or authorization attempts are registered. The authentication token may be locked (and unlocked) according to token specific rules.

In addition access to the Private Key may be locked independently, e.g. if several tokens are connected to the Private Keys and the number of consecutive unsuccessful authorization attempts reaches a threshold, the access to the Private Key may be locked. In this case, a new verification of Subject identity according to 3.3.2 is required to unlock the access to the Private Key.

6.4.3 Other aspects of activation data

Activation Data MAY be distributed to the Subject separately from the Signature Creation Device.
Activation Data MAY be distributed using a distribution service requiring verification of Subject identity.

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 natural persons (QCP-n) of ETSI EN 319 411-2 [14].

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 detection 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. Also see 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 natural persons (QCP-n) of ETSI EN 319 411-2 [14]

Se 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 [9] 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 natural persons (QCP-n) of ETSI EN 319 411-2 [14].

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 [16] 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 [7] or IETF RFC 5280 [2].

Certificate profiles SHALL be in accordance with the SEID profile for certificates issued to natural persons [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 [7] 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 [15].

7.3.1 Version number(s)

7.3.2 OCSP extensions

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

Compliance audits SHALL be conducted regularly.

Buypass is audited for compliance against ETSI EN 319 401 [12], ETSI TS 319 411-1 [13] and ETSI EN 319 411-2 [14].

As a result, Buypass has received, and will continue to maintain, a seal of assurance for CAs.

If the results of an audit report recommend corrective action, Buypass will develop and initiate a corrective action plan.

The result of the most recent compliance audit is posted on Buypass Web.

For topics not covered by this external audit, Buypass annually performs internal audits.

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

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 Qualified 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 for Buypass Class 3 Qualified Certificates are published on Buypass Web. These fees are subject to change, and any such changes are notified at least 14 days before the fees become effective.

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 Subject or Subscriber 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 [19], [24] and [25].

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.

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 Buypass Class 3 Qualified Certificates SHALL be the property of the respective Subscriber named in these 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 Buypass Class 3 Qualified 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 obligations.

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 for Buypass Class 3 Qualified Certificates [17] and the Certification Practice Statement for Buypass Class 3 Qualified Certificates [18].

9.6 Representations and warranties

Buypass operates as both the CA and RA for all Certificates issued under the Certificate Policy [17] and thereby fulfills all CA and RA obligations in this section.

9.6.1 CA Representations and Warranties

a) The CA SHALL provide the following services:
- registration service
- certificate generation service
- dissemination service
- revocation management service
- revocation status service
- subject device provision service

Buypass offers all of the above services.

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

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

The registration service may be subcontracted to the Subscriber, i.e. when the Subscriber is different from the Subject. This may be the case for organizations issuing Certificates to their employees. In such situations, the revocation management service may also be subcontracted to the Subscriber.

Certificates may be issued on smart cards issued by another Card Issuer than Buypass. In this case, parts of the registration service (i.e. Subject Identification) may be subcontracted to the Card Issuer for Subjects registering for smart cards issued by the Card Issuer.

The Private Key associated with the Public Key in a Certificate is always protected within a Signature Creation Device (SCDev), either in the form of a smart card or an HSM. In case of smart card, the subject device provision service may be subcontracted to a Card Bureau.

The distribution of a smart card and/or Activation Data may be subcontracted to a Distribution Service Provider. The Distribution Service Provider may be responsible for verifying the identity of the Subject as described in 3.2 at time of delivery.

c) The CA SHALL be responsible for providing its services in conformance with the Certificate Policy for Buypass Class 3 Qualified Certificates [17] and consistent with the Certification Practice Statement for Buypass Class 3 Qualified Certificates [18], even when functionality is undertaken by Subcontractors.

See 8

d) 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 Qualified Certificates to persons identified in association with it (as a subject). Since Buypass also performs all RA tasks for these Certificates, this is an acceptable exception from this requirement conflict of interest.

e) 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 Certificates

f) 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

A Subscriber may operate as a Local Registration Authority (LRA) and must fulfill the relevant RA obligations in accordance with the Subscriber Agreement.

A Distribution Service Provider may be used to verify the identity of the Subject at time of delivery. In this case the Distribution Service Provider performs parts of the RA functions. However, the Distribution Service Provider is not operating as an RA as such.

The RA SHALL:

- receive Certificate applications from Subjects and Subscribers, both initial applications (see 4.1.1.1 and 4.1.1.2) and rekey applications (see 4.6.3.1 and 4.6.3.2)
- verify all information submitted by Subjects and 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 Certificate
- receive and verify requests from Subjects and Subscribers for the revocation of Certificates, and if the verification of a revocation request is successful, submit a request to the CA for the revocation of such Certificate
- notify Subjects that a Certificate has been issued
- notify Subjects and Subscribers that a Certificate has been suspended, revoked or will soon expire

9.6.3 Subscriber Representations and Warranties

9.6.3.1 Subject obligations

The Subject SHALL ensure that all obligations of the Subject Agreement are fulfilled.

The Subject may explicitly authorize a Partner to submit the Certificate application on behalf of the Subject. The Partner may handle both initial applications and rekey applications for one or more Subjects.

The Partner is identified with its Organization Number and name as registered in the Central Coordinating Register for Legal Entities. The Partner will register National Identification Number, name and contact information of the natural persons authorized to take the roles as Authorized Partner Representatives.

The Partner is responsible for submitting accurate and complete information to the CA based on information provided by the Subject. All other obligations are solely for the Subject to fulfill.

The Subject SHALL:

- submit accurate and complete information to the CA in accordance with the requirements in the Certification Practice Statement for Buypass Class 3 Qualified Certificates [18].
- ensure that the Private Keys and Certificates are only used in accordance with any limitations notified to the Subscriber
- exercise reasonable care to avoid unauthorized use of the Subject Private Keys, particularly the Subject SHALL keep the Activation Data to himself/herself
- request the Certificate to be revoked when a valid revocation reason exists (see 0)
- 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

9.6.3.2 Subscriber obligations

The Subscriber SHALL ensure that all obligations of the Subscriber Agreement are fulfilled. If the Subscriber and Subject are separate entities, the Subscriber SHALL make the Subject aware of those obligations applicable to the Subject (as listed in 9.6.3.1).

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 Qualified Certificates [18]
- 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 0).
- inform the CA whenever an Authorized Subscriber Representative no longer is authorized to represent the Subscriber
- in the case of being informed that the CA has been compromised, ensure that the Private Key is no longer used.

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 Qualified Certificates [17].

The Relying Party SHALL:

- restrict reliance on Buypass Class 3 Qualified Certificates to the purposes for those Certificates as defined by 1.4
- acknowledge applicable terms, conditions, warranties and liability caps as defined in 9.2
- rely on a Buypass Class 3 Qualified 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 Qualified Certificate and the value of any transaction that may involve the use of a Buypass Class 3 Qualified 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 Qualified Certificates, including use of revocation services, in accordance with best practice certification path validation as defined by RFC 5280 [2]
- take into consideration all information in the Certificate, in this Policy and obey best practices for validating signatures (see for example [23])

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 fulfill all obligations as defined by the respective Subcontractor agreement, including the implementation of any controls required by the CA.

The Subscriber Agreement is used as a Subcontractor agreement whenever the Subscriber is operating as a Local Registration Authority (LRA).

The subject device provision services subcontracted to a Card Bureau is regulated within a Card Bureau service agreement.

Similarly, the services subcontracted to a Card Issuer are regulated within agreements between the Card Issuer and Buypass.

The services provided by a Distribution Service Provider for secure distribution of the smart card and/or Activation Data are commercial services with security controls, liability and a quality of service that are not subject to special regulations from Buypass.

A legal person acting as a Partner must have a contractual relationship with Buypass. However, the Partner is not acting directly as a subcontractor for Buypass, but as a representative for the Subject.

9.7 Disclaimers of warranties

Issuance of Certificates in accordance with the Certificate Policy [17] SHALL NOT make the CA an agent, fiduciary, trustee, or other representative of Subscribers or Relying Parties

9.8 Limitations of liability

Any limitations of liability SHALL be according to Norwegian law and SHALL be described in respective Subject or Subscriber Agreements.

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

The CA has defined the following yearly liability caps for:

- **Subscribers and Relying Parties:** NOK 5.000,- per transaction limited to NOK 10.000,- for the aggregate of all digital signatures and transactions related to a given Subject per year
- **Relying Parties:** NOK 50.000,- for all digital signatures and transactions related to all Certificates for a given Relying Party per year

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, Subject Agreements, 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

Indemnification by Subjects:
To the extent permitted by applicable law, Subjects 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 Qualified Certificate or any service provided in respect to Buypass Class 3 Qualified Certificates for:

- the Subject's failure to perform the obligations of a Subject as defined in 9.6.3.1
- falsehood or misrepresentation of fact by the Subject on the Subject's Certificate application
- failure by the Subject 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 Subject's failure to protect the Subject Private Key, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subject Private Key

The applicable Subject Agreement MAY include additional indemnity obligations.

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 Class 3 Qualified Certificate or any service provided in respect to Buypass Class 3 Qualified Certificates for:

- the Subscriber's failure to perform the obligations of a Subscriber as defined in 9.6.3.1
- 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 applicable Subscriber Agreement MAY include additional indemnity obligations.

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 Qualified Certificate or any service provided in respect to Certificates for the Relying Party's failure to perform the obligations of a Relying Party as defined in 9.6.4

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 [17] or the Certification Practice Statement [18] 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. Also see 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 [17] or the Certification Practice Statement [18] with 15 days advance notice.

Any change that may materially influence users of the Certificate Policy [17] or the Certification Practice Statement [18] 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[17] or the Certification Practice Statement [18] that is amended SHALL be subject to a new advance notice.

Modifications to either the Certificate Policy [17] or the Certification Practice Statement [18] 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 [17] or the Certification Practice Statement [18] 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

Any dispute arising out of or in respect to any Buypass Class 3 Qualified Certificate or any services provided in respect to any Buypass Class 3 Qualified Certificate that is not resolved by alternative dispute resolution SHALL be brought 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 [17], the Certification Practice Statement [18], 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 [17] or the Certification Practice Statement [18] 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 Qualified Certificates issued for the remainder of the validity periods of such Certificates, also upon termination or expiration of the Certificate Policy [17], the Certification Practice Statement [18], 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 [17] the Certification Practice Statement [18], 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