CERTIFICATION PRACTICE STATEMENT

BUYPASS CLASS 2 MERCHANT CERTIFICATES

Effective date: 28.04.2014

PUBLIC

Version: 2.0
Document date: 15.03.2014

Buypass AS
Nydalsveien 30A, PO Box 4364 Nydalen
N-0402 Oslo, Norway
Tel.: +47 23 14 59 00
Fax: +47 23 14 59 01
E-mail: kundeservice@buypass.no
VAT: NO 983 163 327
www.buypass.no

Table of content

DEFINITIONS

Terms	Definition
Activation Data	Data that gives access to the Private key.
Authorized Subscriber Representative	A natural person who has express authority to represent the Subscriber.
Buypass	Buypass AS, registered in the Norwegian National Register of Business Enterprises with organization number 983 163 327.
Buypass Merchant	Private and public enterprises using Buypass Nett directly or through an integration partner.
Buypass Nett	Centralized IT solution owned and operated by Buypass. Buypass Nett grants Buypass Merchants access to Buypass ID services and net based payment services.
Central Coordinating Register for Legal Entities (“Enhetsregisteret”)	Norwegian 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 such as the National Register of Business Enterprises.
Certificate	Public key of a user, together with other information, rendered unforgeable by encipherment with the Private Key of the certificate authority which issued it (see ITU-T Recommendation X.509). In this document the term is used synonymously with Buypass Class 2 Merchant Certificate.
Certificate Applicant	Authorized Subscriber Representative who has privileges to submit a Certificate application on behalf of the Subscriber.
Certificate Application	A Subscriber's application for a Merchant Certificate.
Certificate Authority (CA)	Authority trusted by one or more users to create and assign Certificates.
Certificate Policy (CP)	Named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements (see ITU-T Recommendation X.509).
Certificate Rekey	The issuance of a new Certificate for a previously registered Subscriber based on a new key pair. This includes routine rekey, rekey prior to expiration and rekey after revocation.
Certificate Renewal	The issuance of a new Certificate for a previously registered Subscriber based on an existing Certificate without changing the Subscriber’s Public Key.
Certificate Status Service	Revocation Status Service as defined in section 2.1.1.
Certification Practice Statement (CPS)	Statement of the practices which a Certificate Authority employs in issuing Certificates (see [1]).
Contract Signer	Authorized Subscriber Representative who has authority on behalf of Subscriber to sign Subscriber Agreements.
Distribution Key	Secret key that protects access to CA generated Subject Private keys during key distribution from CA to Subject Sponsor.
Merchant Agreement	Signed contractual agreement between Buypass and legal entity giving the legal entity access to be a Buypass Merchant in Buypass Nett.
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 Authorized Subscriber Representatives on behalf of one or more Subscribers through the initial Subscriber Registration. The legal person must have signed a Contractual agreement with Buypass before acting as a Partner.

Terms	Definition
Private Key	The key of a key pair that is kept secret by the holder of the key pair, being 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.
Registration Authority (RA)	Registration authorities, i.e., the entities that establish enrollment procedures for end-user Certificate Applicants, perform identification and authentication of Certificate Applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA.
Relying Party	Recipient of a Certificate who acts in reliance on that Certificate and/or digital signatures verified using that Certificate (see [1]).
Signing Authority	Authorization to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Subscriber.
Subcontractor	Party providing services on behalf of the CA.
Subject	Application or system which is the holder of the Private Key associated with the Public Key given in the Certificate.
Subject Key Provision Service	A service that generates the Subject's key pair and distributes the Private key to the Subject.
Subject Sponsor	Authorized Subscriber Representative who has privileges to undertake the Subject's obligations under this policy whenever the Subject is a non-human entity.
Subscriber	Organization subscribing with a Certificate Authority on behalf of one or more Subjects.
Subscriber Agreement	Contractual agreement or written statement that specifies all Subscriber obligations under this policy.

REFERENCES

[1] IETF RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practises Framework – 1999.
[2] FIPS PUB 140-1: "Security Requirements for Cryptographic Modules".
[3] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".
[4] SEID prosjektet leveranse oppgave 1 Anbefalte Sertifikatprofiler for personsertifikater og virksomhetssertifikater, versjon 1.01.
[5] Buypass Class 2 Certificate and CRL profiles, current version
[6] Policy for sikkerhet i Buypass, versjon 1.01 1.4.2003.
[7] ISO/IEC 27002:2005: Information technology - Security techniques. Code of Practice for Information Security Management.
[8] ETSI TS 102 042 - Policy requirements for certification authorities issuing public key certificates
[9] ETSI TS 102 176 - Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
[10] CEN Workshop Agreement 14167-2: 2004: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)".
[11] CEN Workshop Agreement 14167-3: 2004: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)".
[12] CEN Workshop Agreement 14167-4: 2004: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP".
[13] ISO/IEC 15408 (parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security".
[14] Certificate Policy for Buypass Class 2 Merchant Certificates, current version
[15] IETF RFC 2560 Internet X.509 PKI Online Certificate Status Protocol (OCSP), June 1999
[16] Lov 15.juni 2001 nr.81 om elektronisk signatur
[17] Lov 14.april 2000 nr.31 om behandling av personopplysninger (personopplysningsloven)
[18] Forskrift 15.des 2000 nr.1265 om behandling av personopplysninger (personopplysningsforskriften)
[19] Certification Practice Statement for Buypass Class 2 Merchant Certificates, this document
[20] IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.
[21] AICPA/CICA, WebTrust Program for Certification Authorities, version 1.0, 25.august 2000

1 Introduction

1.1 Overview

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

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

This document provides a Certification Practice Statement for Buypass Class 2 Merchant Certificates.

Buypass is the Certificate Authority (CA) for all Buypass Class 2 Merchant Certificates.

Buypass Class 2 Merchant Certificates may only be issued to organizations that are registered in the Central Coordinating Register for Legal Entities.

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

The Subject denotes a non-human entity (application or system) that represents the Subscriber and which is the holder of the Private Key associated with the Public Key to which the Certificate is issued. The Subject shall be represented by a natural person in the role of a Subject Sponsor who undertakes the Subject’s obligations as defined in the Certificate Policy for Buypass Class 2 Merchant Certificates [14].

1.1.1 How to read this document

Text that is outside text boxes is the original text from the Certificate Policy for Buypass Class 2 Merchant Certificates [14]. All Certificate Policy requirements contain either a SHALL, SHALL NOT, SHOULD, SHOULD NOT or MAY statement.

Text contained inside blue colored 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 Registration Authority (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 2 Merchant Certificates.

1.2 Identification

The Certificate Policy for Buypass Class 2 Merchant Certificates has been provided the following Certificate Policy Identifier / OID; 2.16.578.1.26.1.2.5.

Relying Parties will recognize a particular Certificate as having been issued under [14] by inspecting the Certificate Policies extension field of the Certificate, which then shall hold the policy OID above.

The same Buypass CA that is used to issue Class 2 Merchant Certificates also issue Certificates under the following Certificate Policies / OIDs:

- Certificate Policy for Buypass Domain Plus SSL Certificates - OID 2.16.578.1.26.1.2.3
- Certificate Policy for Buypass Domain SSL Certificates - OID 2.16.578.1.26.1.2.4
- Certificate Policy for Buypass Class 2 (Personal) Certificates - OID 2.16.578.1.26.1.2.1

1.3 Community and applicability

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

1.3.1 Applicability

Buypass Class 2 Merchant Certificates are applicable for supporting PKI based security services between Buypass Merchants and Buypass. In particular, the Certificates can be used to:

- authenticate the identity of a Buypass Merchant
- encrypt data for an organization or to exchange symmetric keys to be used for encryption

A Subscriber under this policy MUST be an organization that is registered in the Central Coordinating Register for Legal Entities. A Subject under this policy MUST be an application or system that represents, and operates on behalf of the Subscriber.

1.4 Contact details

Buypass Policy Board is responsible for the Certificate Policy for Buypass Class 2 Merchant Certificates [14] and Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] and their maintenance.

Contact point for questions regarding these documents is:

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

Telephone: + 47 22 70 13 00
Fax: + 47 23 14 59 01
Email: policy@buypass.no

Contact point for all other matters concerning Buypass Class 2 Merchant Certificates is:

Buypass Kundeservice
Postboks 639
N-2810 Gjøvik

Telephone: + 47 22 70 13 00
Fax: + 47 61 13 58 50
Email: kundeservice@buypass.no

2 General provisions

2.1 Obligations

Buypass operates as both CA and RA for all Certificates issued under the Certificate Policy for Buypass Class 2 Merchant Certificates [14] and thereby fulfills all CA and RA obligations in this section.

2.1.1 CA obligations

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

- registration service
- certificate generation service
- dissemination service

- revocation management service
- revocation status service

Buypass offers all the above CA and RA services.

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

The CA MAY provide a Subject key generation and Subject Key Provision Service.

Buypass provides both a Subject key generation service and a Subject Key Provision Service.

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

Buypass allows external RAs to be established. A prerequisite is that they are capable to operate in conformance with the Certificate Policy for Buypass Class 2 Merchant Certificates [14]. Necessary conformance assessments are handled case by case.

The CA SHALL be responsible for providing its CA and RA services in conformance with the Certificate Policy for Buypass Class 2 Merchant Certificates [14] and consistent with the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19], even when functionality is undertaken by Subcontractors.

See section 2.7

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

The CA SHALL warrant that an issued Certificate is linked to one (1) unique organization registered in the Central Coordinating Register for Legal Entities.

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

If the Subject's Private Key is generated by the CA, the CA SHALL provide the Subject with means to protect the Private Key.

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

2.1.2 RA obligations

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

The RA SHALL:

- receive Certificate Applications from Subscribers, both initial applications (see 4.1.1) and rekey applications (see 4.1.2)
- verify all information submitted by Subscribers, both for initial applications and for rekey applications and if such verification is successful, submit a request to the CA for the issuance of a Buypass Class 2 Merchant Certificate
- receive and verify requests from Subscribers for the revocation of Buypass Class 2 Merchant Certificates, and if the verification of a revocation request is successful, submit a request to the CA for the revocation of such Certificate
- notify Subscribers that a Buypass Class 2 Merchant Certificate has been issued to them
- notify Subscribers that a Buypass Class 2 Merchant Certificate issued to them has been suspended, revoked or will soon expire

2.1.3 Subscriber obligations

The Subscriber SHALL fulfill all obligations of the Subscriber Agreement.

The Subscriber SHALL:

- submit accurate and complete information to the CA in accordance with the requirements in the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19]
- maintain correct information about the Subscriber and Subject, and notify the RA or CA of any changes to this information
- request the Certificate to be revoked when a valid revocation reason exists (see 4.4.1)
- be responsible for ensuring that restrictions on Private Keys and Certificates use are maintained
- exercise reasonable care to avoid unauthorized use of the Subjects Private Keys
- inform the RA 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 by the Subject
- inform Certificate Applicant and Subject Sponsors of all obligations applicable to the Subject

2.1.4 Subcontractor obligations

The CA SHALL have a properly documented agreement and contractual relationship in place where the provision of services (see 2.1.1) 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.

Not applicable.

2.1.5 Relying Party obligations

A Relying Party is solely responsible for deciding whether or not to rely on Certificates issued under the Certificate Policy for Buypass Class 2 Merchant Certificates [14].

The Relying Party SHALL:

- restrict reliance on Buypass Class 2 Merchant Certificates to the purposes for those Certificates as defined by section 1.3
- acknowledge applicable terms, conditions, warranties and liability caps as defined in section 2
- rely on a Buypass Class 2 Merchant 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 2 Merchant Certificate and the value of any transaction that may involve the use of a Buypass Class 2 Merchant 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 2 Merchant Certificates, including use of revocation services, in accordance with best practice certification path validation as defined by RFC 5280 [20]

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

2.2 Liability

Any limitations of liability SHALL be according to Norwegian law and SHALL be described in respective 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

- **for 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.

2.3 Financial responsibility

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

2.3.1 Indemnification of CA and RA by Relying Parties

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 2 Merchant Certificate or any service provided in respect to Buypass Class 2 Merchant Certificates for:

- the Subscriber's failure to perform the obligations of a Subscriber as defined in section 2.1.3
- falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application
- failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party
- the Subscriber's failure to protect the Subscriber's Private Key, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's Private Key
- the Subscriber's use of a name (including without limitation within a common name) that infringes upon the Intellectual Property Rights of a third party

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 2 Merchant Certificate or any service provided in respect to Buypass Class 2 Merchant Certificates for:

- the Relying Party's failure to perform the obligations of a Relying Party as defined in section 2.1.5

The applicable Subscriber Agreement MAY include additional indemnity obligations.

2.3.2 Fiduciary relationships

Issuance of Certificates in accordance with the Certificate Policy for Buypass Class 2 Merchant Certificates [14] SHALL NOT make the CA an agent, fiduciary, trustee, or other representative of Subscribers or Relying Parties.

2.3.3 Administrative processes

No stipulations.

2.4 Interpretation and enforcement

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

2.4.1 Governing law

The laws of the country of Norway SHALL govern the construction, validity, interpretation, enforceability and performance of the Certificate Policy for Buypass Class 2 Merchant Certificates [14], the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] and all related Subscriber Agreements.

2.4.2 Severability, survival, merger, notice

Severability
In the event that a clause or provision of the Certificate Policy for Buypass Class 2 Merchant Certificates [14] or the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] 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 Buypass Class 2 Merchant Certificates issued for the remainder of the validity periods of such Certificates, also upon termination or expiration of the Certificate Policy for Buypass Class 2 Merchant Certificates [14], the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] or any Subscription Agreement.

Merger
The Rights and Obligations of Buypass as CA or 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 for Buypass Class 2 Merchant Certificates [14], the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] or a Subscription Agreement SHALL be given in writing (e-mail, facsimile, post, courier) to the contact point specified in section 1.4.

Any notice to be given by Buypass under the Certificate Policy for Buypass Class 2 Merchant Certificates [14], the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] or any Subscription Agreement SHALL be given in writing (by e-mail, by facsimile, by post or by courier) to the last address, email address or facsimile number for the Subscriber on file with Buypass.

2.4.3 Dispute resolution procedures

Any dispute arising out of or in respect to any Buypass Class 2 Merchant Certificate or any services provided in respect to any Buypass Class 2 Merchant 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.

2.5 Fees

No stipulation.

2.6 Publication and repositories

The Certificate Policy for Buypass Class 2 Merchant Certificates [14] and the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] SHALL be publicly available on the Buypass web (www.buypass.no) 24 hours a day 7 days per week (24x7).

The Certificate Policy for Buypass Class 2 Merchant Certificates [14] and the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] are published on the Buypass web (www.buypass.no).

Certificates and Revocation status information are available at the location(s) specified in the appropriate fields of the Certificate.

Every Class 2 Merchant Certificate issued by Buypass contains a CRL distribution point Certificate extension that contains a URL for CRL retrieval and an Authority Information Access Certificate extension that contains a URL for OCSP service access. Both Certificate revocation status services are available 24x7 and available on the Buypass web (www.buypass.no).

Certificates issued by Buypass are available through the LDAP protocol. The URL is included in the CRL Distribution Point extension of Class 2 Merchant Certificates. The LDAP service is available 24x7 and available on the Buypass web (www.buypass.no).

2.7 Compliance audit

a) The CA SHALL be audited annually for compliance with the practices and procedures set forth in the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19].

Buypass undergoes at least one annual compliance audit by an independent licensed 3rd. party auditor against the practices and procedures set by this document.

The scope of the annual internal audit also partly includes the different practices and procedures.

If the results of an audit report recommend corrective action, Buypass will develop and initiate a corrective action plan as a part of the Information Security Management System.

2.8 Confidentiality policy

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

The following information is not considered confidential or private:
- certificates
- certificate 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 [16], [17] and [18].

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

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

c) 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 laws of Norway in all matters concerning release of confidential information to law enforcement officials.

2.9 Intellectual property right

a) Key pairs corresponding to Buypass CA Certificates SHALL be the property of Buypass. Key pairs corresponding to Class 2 Merchant Certificates SHALL be the property of the respective Subscriber of those Certificates.

b) Buypass SHALL retain all Intellectual Property Rights in and to the Certificates and revocation information that it issues except for any information that is supplied by a Subscriber and that is included in a Class 2 Merchant Certificate, which information SHALL remain the property of the Subscriber. Buypass and Subscribers grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that the use of Certificates is subject to their purpose as defined by section 1.3.

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 2 Merchant Certificates [14] as well as the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19].

3 Identification and authentication

3.1 Initial registration

3.1.1 Identification/authentication of Subscriber and Subscriber Representatives

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

- the Subscribers' Organization Number and Name as defined in the Central Coordinating Register for Legal Entities
- the name and contact information of all Subscriber representatives authorized to operate as Contract Signer, Certificate Applicant or Subject Sponsor

As a part of initial Subscriber Registration, the Subscriber registers the following mandatory information with Buypass:

- the Subscriber's Organization Number and Organization Name as registered in the Central Coordinating Register for Legal Entities
- name and contact information for the Contract Signer
- name and contact information of the Certificate Applicant and Subject Sponsor or
- a Partner's Name for one or both of the roles Certificate Applicant or Subject Sponsor

All information registered is incorporated into a Subscriber Agreement that is signed and thereby confirmed by the Contract Signer. If the Subscriber wants to add, remove or change registered Subscriber information, the Subscriber needs to go through a new "Subscriber Registration and Subscriber Agreement Signing" step (see section 4.1.1).

The Partner will register Name and contact information of the natural persons authorized to take the roles Certificate Applicant and Subject Sponsor before a Certificate Application has been registered.

a) All information provided SHALL be verified according to section 4.1.1.

All Subscriber information has to be successfully verified according to section 4.1.1 before a Certificate Application is approved.

3.1.2 Authorization of Subscriber Representatives

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

The same person MAY fill one, two or all three roles at the same time.

a) A Contract Signer's **Signing Authority** SHALL be established through:
   - independent confirmation from the Subscriber that the person is an employee or an agent of the Subscriber

The Contract Signer may be the same person who signed the Merchant Agreement. In this case, the Merchant Agreement Signing Authority is accepted as Signing Authority for the Subscriber Agreement.

If the Contract Signer is not the same person who signed the Merchant Agreement, Buypass contacts the Subscriber (typically the switchboard, the HR department or an independent person) to obtain an independent confirmation that the Contract Signer is an employee or an agent of the Subscriber.

b) A Certificate Applicant's **Certificate Application Authority** SHALL be established through:
   - an express authorization statement issued by an authorized Contract Signer

The Contract Signer explicitly authorizes a Certificate Applicant through the signed Subscriber Agreement.

The Contract Signer may authorize a Partner to act as a Certificate Applicant.

c) Proof of authorization for a Subject Sponsor SHALL be established through:
   - an express authorization statement issued by an authorized Contract Signer

The Contract Signer explicitly authorizes a Subject Sponsor through the signed Subscriber Agreement.

The Contract Signer may authorize a Partner to act as a Subject Sponsor.

d) The CA and the Subscriber enters into a written Subscriber Agreement, whereby, for a specified term, Subscriber expressly authorizes one Certificate Applicant and one Subject Sponsor designated in such agreement to exercise this Authority with respect to future Certificate issuance on behalf of the Subscriber.

As part of the Subscriber Registration process (see 4.1.1), the Subscriber enters into a Subscriber Agreement with Buypass. This Subscriber Agreement expressly authorizes one Certificate Applicant and one Subject Sponsor to exercise this Authority with respect to future Certificate issuance on behalf of the Subscriber.

In this case, the Subscriber Agreement provides that the Subscriber is obligated under the Subscriber Agreement for all Certificates issued to the Subscriber until their authority is revoked.

3.2 Certificate Rekey

The requirements for identification and authentication of Subscriber and Authorized Subscriber Representatives are the same as for initial registration (see 3.1).

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 before a rekey, the statements in 3.1 apply.

3.3 Revocation requests

The requirements for identification and authentication of originators of revocation requests are described in section 4.

4 Operational requirements

4.1 Certificate Application

A Certificate Application is implicitly included in the Subscriber registration. Routine rekey application and subsequent issuance are automatically processed in due time before the Certificate expires. This does not require an explicit Certificate Application from the Subscriber. A rekey application may be explicitly requested from the Certificate Applicant.

4.1.1 Initial application

The initial application is implicitly included in the Subscriber registration and Subscriber Agreement signing.

The Subscriber must register with Buypass all Subscriber information defined in section 3.1.1 as well as any required proof of authorization for the registered Certificate Applicant and Subject Sponsor as described in 3.1.2.

a) The Certificate Applicant and Subject Sponsor MUST register with an RA as Authorized Subscriber Representatives either prior to, or at the time of, applying for a Certificate. Section 3.1 defines necessary requirements for identification and authorization.

The Certificate Applicant and Subject Sponsor are registered as part of the Subscriber registration which implicitly includes the initial Certificate Application.

b) The Subscriber SHALL provide to the RA:
- all Subscriber information as defined in section 3.1
- the Subscriber's explicit consent to all terms and conditions regarding the use of the Certificate as defined in the Subscriber Agreement

No Certificate is issued by Buypass before all information above has been provided by the Subscriber as part of the Subscriber Agreement.

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

Not applicable

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

Buypass does not use external RAs.

e) The procedure of verifying the Certificate Application performed by the RA or CA SHALL ensure:
- that the Certificate Application is accurate, complete and duly authorized
- that the submitted Subscriber information has been verified against the relevant registers such as for example the Central Coordinating Register for Legal Entities

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

- all mandatory Subscriber information (see 3.1) has been obtained from the Subscriber
- the Subscriber's Organization Name and Organization Number exist in the Central Coordinating Register for Legal Entities
- the Contract Signer is an employee or an agent of the Subscriber
- authorization has been established for the Certificate Applicant and Subject Sponsor, see section 3.1.2

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

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

The Certificate Applicant is notified by phone or e-mail whenever the Certificate Application is rejected.

4.1.2 Rekey application

The requirements in section 4.1.1 SHALL apply also to a rekey application. However, routine rekey applications are handled and processed automatically.

Buypass notifies the Certificate Applicant by e-mail with information that an existing Certificate is about to expire at the latest eight weeks before the expiry date.

A routine rekey application is automatically initiated at the latest four weeks before the Certificate's expiry date. The Certificate Application is processed without any action required from the Subscriber.

Buypass sends the new Certificate and Activation Data to the registered Certificate Applicant and Subject Sponsor.

Other rekey applications (e.g. after revocation) must be applied from or confirmed by the registered Certificate Applicant according to defined procedures.

Certificate Renewal is not supported.

4.2 Certificate issuance

Two different schemes for Certificate issuance are supported dependent on whether:

- the Subject's key pair is generated by the CA
- the Subject's key pair is generated by the Subscriber

Only CA generated Subject keys is currently supported.

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.

All Subject key pairs are generated on trusted servers within Buypass secure production facilities (see 5.1). The process ensures that Private Keys are kept confidential at all times and that the only party that has access to the Private Keys after they have been generated is the Subscriber of the issued Certificate.

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

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

c) If the CA generates the Subject's key pair:
   - 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 passed to the registered Subject Sponsor;

Key generation and Certificate issuance are performed in one operation. Regarding secure Private Key distribution, see 6.1.2.

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

Not applicable.

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

Not applicable.

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

All Class 2 Merchant Certificates issued follow the Certificate profile requirements defined in section 7.

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

Every Class 2 Merchant Certificate issued is distributed to the Subscriber by attaching it to an e-mail sent to the registered Certificate Applicant.

In addition, all Class 2 Merchant Certificates issued are made publicly available to Relying Parties through a public LDAP directory service. The URLs are included in the CRL Distribution Point extension of all Class 2 Merchant Certificates issued and are available on the Buypass web (www.buypass.no).

4.3 Certificate acceptance

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

The Subscriber is given a 2 weeks verification period to verify the Certificate and to notify Buypass if any of the information parameters are incorrect.

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

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

4.4 Certificate suspension and revocation

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 24x7.

Buypass offers a 24x7 revocation service where Subscribers can submit revocation requests either by phone, e-mail or the Buypass web (www.buypass.no).

b) The maximum delay between receipt of a revocation request and the change to revocation status information being available to all Relying Parties SHALL not exceed 24 hours.

The revocation grace period (time between receipt of the revocation request and consequent start of processing by the CA) is 1 hour.

Unless the certificate request processing concludes that the revocation request is rejected, the Certificate will either be revoked or suspended (see 4.4.5) at the latest within 24 hours after the revocation request was received.

For Relying Parties that depend on the Buypass OCSP service, information about the suspension or revocation is available immediately after the Certificate has been suspended or revoked.

Relying Parties that depend on the Buypass CRL service will be informed about the suspension/revocation as soon as the next CRL is published. The next CRL will be published no later than 24 hours after receipt of the revocation request.

c) Revocation status information SHALL be available 24x7. 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 for longer than a maximum period of time as denoted in the certification practice statement.

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

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

Service information that is considered relevant for Subscribers and/or Relying Parties is published on the Buypass web (www.buypass.no)

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

Buypass offers revocation status information for every Class 2 Merchant Certificate for as long as the Certificate is valid.

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

The registered Certificate Applicant for a specific Class 2 Merchant Certificate is notified by e-mail once the Certificate has either been revoked or suspended.

4.4.1 Circumstances for revocation

A Certificate SHALL be revoked if:

- the Subscriber requests revocation of its Class 2 Merchant Certificate
- the Subscriber indicates that the original Certificate Application was not authorized and does not retroactively grant authorization
- the CA obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Class 2 Merchant Certificate) has been compromised, or that the Certificate has otherwise been misused
- the Subscriber terminates it's use of the Subject Private Key while the corresponding Public Key Certificate is still valid
- the CA receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement
- the CA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate
- a determination, in the CA's sole discretion, that the Certificate was not issued in accordance with the terms and conditions of the Certificate Policy for Buypass Class 2 Merchant Certificates [14]
- 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 arranged for another CA to provide revocation support for the Certificate
- the Private Key of the Subordinate CA used for issuing that Certificate is suspected to have been compromised
- the Subscriber ceases to exist
- the Merchant Agreement is terminated

4.4.2 Who can request revocation?

a) Only Authorized Subscriber Representatives are authorized to request Certificate revocation on behalf of the Subscriber.

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

Buypass accepts Revocation Requests from previously unregistered Subscriber representatives only if:
(i) the revocation request is confirmed by an existing Authorized Subscriber Representative
(ii) Buypass, through further investigation, has reason to believe that a valid revocation reason exists (see 4.4.2 b)

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

Buypass is entitled to, and will revoke a Subscriber's Class 2 Merchant Certificate, at any time for any of the reasons set forth in section 4.4.1.

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

If a revocation request is received and if Buypass is not able to establish the requestor as an Authorized Subscriber Representative, Buypass will make an effort to investigate whether there is a valid revocation reason.

4.4.3 Procedure for revocation request

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

Buypass offers a 24x7 revocation service where Subscribers can submit revocation requests by phone, e-mail or the Buypass web (www.buypass.no). Contact points for revocation are communicated to the Subscriber through the Subscriber Agreement and are available on the Buypass web (www.buypass.no).

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 will operate according to documented routines. The routines describe the different controls that need to be executed before the request is authorized and revocation is performed.

4.4.4 Revocation request grace period

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

b) For revocation reason "key compromise", see section 4.4.15.

4.4.5 Circumstances for suspension

a) If an RA is not able to process a Certificate revocation request in due time (see 4.4 b), the Certificate SHALL be suspended until the revocation request has been properly processed.

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

4.4.6 Who can request suspension

a) Certificate suspension can only be requested by an RA.

4.4.7 Procedure for suspension request

a) The RA SHALL submit a suspension request to the CA whenever the criteria for suspension are fulfilled (see 4.4.5).

A revocation request submitted outside the opening hours of the regular Buypass Kundeservice is directed to a standby service with authority to suspend the Certificate after reasonable assurance has been established that the request originates from an authorized source.

4.4.8 Limits on suspension period

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

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

4.4.9 CRL issuance frequency

a) The CA SHALL provide a CRL service.

Buypass provides a CRL service where CRLs may be accessed using either the HTTP protocol or the LDAP protocol. Both URLs are included in the CRL Distribution Point extension of all Class 2 Merchant Certificates that are issued and the URLs are also available on the Buypass web (www.buypass.no).

b) The CRL service 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 every 12th hour. 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.

4.4.10 CRL checking requirements

Relying parties must check either the latest CRL or use the online Revocation status service (4.4.12) in order to establish whether any of the Certificates in the certification path have been revoked.

4.4.11 On-line revocation/status checking availability

a) The CA SHALL provide an on-line revocation status services.

Buypass provides an on-line OCSP service. The service URL is included in the AIA extension of all Certificates and the URL is also available on the Buypass web (www.buypass.no).

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) 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. See also 4.4.9 c)

4.4.12 On-line revocation checking requirements

Relying parties SHALL check either the latest CRL (see 4.4.10) or use the online revocation status service (see 4.4.11) in order to establish whether any of the Certificates in the certification path have been revoked or not.

4.4.13 Other forms of revocation advertisements available

No stipulations.

4.4.14 Checking requirements for other forms of revocation advertisement

No stipulations.

4.4.15 Special requirements regarding key compromise

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

4.5 Security audit procedures

4.5.1 Types of events recorded

The CA SHALL ensure that records of all relevant events and related information regarding the services defined in section 2.1.1 are retained for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.

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

See 4.5.1 b)

b) The foregoing record requirements include, but are not limited to, an obligation to record the following events:
- CA key lifecycle management events, including:
  - key generation, backup, storage, recovery, archival, and destruction
  - cryptographic device lifecycle management events
- CA and Certificate lifecycle management events, including:
  - Certificate Applications, rekey applications and revocation
  - all verification activities required
  - date, time, phone number used, persons spoken to, and end results of verification telephone calls
  - acceptance and rejection of Certificate Applications
  - issuance of Certificates
  - generation of Certificate Revocation Lists (CRLs) and OCSP entries
- security events, including:
  - 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 or RA services and related processes, Buypass ensures that appropriate audit logs are produced that can provide auditable proof of events that is considered to have potential value as evidence in possible future disputes and/or legal proceedings. Audit logging covers, but is not limited to, the events that are listed above. Audit logs retained may be a combination of electronic logs and paper based logs.

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

c) For each log entry, the following elements SHALL be recorded:
- date and time of entry
- identity of the person making the journal entry
- description of entry

See 4.5.1 b)

4.5.2 Frequency of processing log

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.

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.

4.5.3 Retention period for audit log

See section 4.6

4.5.4 Protection of audit log

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

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

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

Only a limited number of persons in trusted roles have access to the audit logs.

4.5.5 Audit log backup procedures

There SHALL be offsite backup of all audit logs.

Buypass performs regular offsite backup of all security relevant audit logs. See also 4.5.4 a)

4.5.6 Audit collection system

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.

4.5.7 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.

4.5.8 Vulnerability assessment

No stipulations.

Audit logging is an integrated 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.

4.6 Records archival

a) Audit records related to service events (see section 2.1.1 for services definition) and that can be of relevance as evidence in legal proceedings concerning a particular Certificate SHALL be retained for at least 10 years after the Certificate either has expired or has been revoked.

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

b) 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.

c) 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 or RA services that Buypass is responsible for (see 2.1.1), 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.

d) 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 section 2.8.

e) The Subscriber SHALL have access to registration information and other information relating to the Subscriber/Subject.

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

4.7 Key changeover

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 section 6.1.5).

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

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

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 section 6.1.4.

See 6.1.4

4.8 Compromise and disaster recovery

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.

a) The CA SHALL define and maintain a business continuity plan (or disaster recovery plan), including planned processes, to act in case of a disaster. The disaster recovery plan SHALL define:
   - a disaster organization
   - if and how the CA will run its operation in the time between the disaster occurs and the time the operation is back to its normal condition
   - the recovery procedures used in case computing resources, software and/or data are corrupted or suspected to be corrupted
   - how a secure environment is re-established
   - the recovery procedure used if the CA Private Key is revoked, how the new CA Certificate is distributed and how the Subjects are recertified

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 or RA services. The disaster recovery plan covers preoperational activities as well as activities taken after a disaster, hereunder off-site recovery of all services if required. Two redundant operations locations are available as well as an off-site disaster recovery location at one of the Buypass premises.

b) Backup of critical CA systems software and hardware SHALL be maintained in order to support timely recovery in case of failure to critical CA system components.

Daily backup is performed to a secondary operations location. All critical CA systems are duplicated to support continuous operation.

c) CA systems data necessary to resume CA operations SHALL be backed up and stored in safe places suitable to allow the CA to timely go back to operations in case of incidents/disasters.

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.

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

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

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

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

f) 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
- revoke any affected Certificates

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

g) 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.

4.9 CA termination

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

a) Before the CA terminates its services the CA SHALL execute the following procedures as a minimum:
- inform the following of the termination: all Subscribers, Relying Parties and other entities with which the CA has agreements or other form of established relations. In addition, this information shall be made available to other Relying Parties
- 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
- 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
- destroy or put beyond use all copies of the CA private signing keys
- revoke unexpired unrevoked Subscriber Certificates, if required

If CA termination is required, Buypass will develop a termination plan that will seek to minimize disruption to Customers, Subscribers, and Relying Parties. Such a termination plan will as minimum ensure that the above procedures are managed.

b) 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 a 3rd party in place for continued operations and fulfillment of obligations in case of bankruptcy.

5 Physical, procedural, and personnel security controls

5.1 Physical security controls

a) Physical access to facilities concerned with Certificate generation, Subject key generation, Subject key provision, and revocation management services SHALL be limited to properly authorized individuals.

Access to Buypass' CA and/or RA facilities is restricted to authorize 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 NOT be left for any significant period without oversight by an authorized person.

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

d) 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 concerned with Certificate generation, Subject key generation, Subject key provision 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 Certificate Service Provider. Relevant prevention and detection mechanisms are in place to address environmental incidents, hereunder power loss, loss of communication, water exposure, fire and temperature changes.

e) 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 control and regular inventory control are designed to prevent and detect unauthorized movement assets.

f) Controls SHALL be implemented to avoid loss, damage or compromise of assets and interruption to business activities.

Buypass maintains procedures for how to securely classify, handle and dispose information and related carriers according to sensitivity.

g) Controls SHALL be implemented to avoid compromise or theft of information and information processing facilities.

See 5.1. e)

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 security and formally appoints personnel to the other trusted roles
- **Security Officer:** is responsible for the implementation of the security practices
- **Security Auditor:** is responsible for controlling that routines are complied with and for reading and maintaining archives and audit logs
- **System Administrator:** is responsible for the operation of the system and installing security software and hardware

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

b) A single person SHALL NOT assume several roles at the same time.

Controls are in place to ensure segregation of duties so that no person can assume several 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 that staffing of qualified personnel is 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 or RA operations is maintained. Risk and vulnerability assessments that are performed regularly include an evaluation of personnel qualifications.

5.2.2 Number of persons required per task

a) Three (3) Security Officers are required to maintain CA Private Keys (generate keys, backup keys, delete keys).

Routines that involve generation, backup or destruction of CA Private Keys ensure that the operations are witnessed by three persons assuming a Security Officer role.

b) One (1) System Administrator and one (1) Security Officer are required to install the cryptographic devices containing CA Private Keys on systems performing CA services.

Routines that involve installation and activation of cryptographic tokens containing CA Private Keys ensure that the operations are performed under dual control (one System Administrator and one Security Officer).

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

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

5.2.3 Identification and authentication for each role

No stipulations.

All personnel assuming one of the trusted roles defined in section 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 or RA facilities (see 5.1) as well as for logical access to CA or RA systems.

5.3 Personnel security controls

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

5.3.1 Background, qualifications, experience, and clearance requirements

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

Buypass' Chief Security Officer has the overall responsibility for 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 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 section 5.2.1. Regarding proof of identity, see 5.2.3.

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

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

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

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

5.3.2 Background check procedures

a) The Security Manager is responsible for ensuring that necessary background checks are completed for all trusted personnel.

See 5.3.1 a)

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

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

5.3.3 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 for refreshment training for personnel assuming trusted roles is evaluated at least once a year by the person responsible for the Buypass Class 2 CA services.

5.3.4 Job rotation frequency and sequence

No stipulations.

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

5.3.5 Sanctions for unauthorized actions

a) Appropriate disciplinary sanctions SHALL be applied to personnel violating the Certificate Policy for Buypass Class 2 Merchant Certificates [14] 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 Certificate Certification Practice Statement for Buypass Class 2 Merchant Certificates [14] 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 any 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 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.

5.3.6 Contracting personnel requirements

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.

5.3.7 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 or RA services as specified in section 2.1.1 are familiar with the Certificate Policy for Buypass Class 2 Merchant Certificates [14] and the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19]. Both documents are available electronically on the Buypass web (www.buypass.no)

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

CA key generation

a) CA key generation SHALL be undertaken in a physically secured environment (see section 5.1) under the control of three (3) Security Officers. The number of personnel authorized to carry out this function shall be kept to minimum.

The CA key ceremony was conducted in the CA operations facilities under control of three Security Officers and under supervision by an independent auditor.

b) The CA private signing key SHALL be generated within a cryptographic device which either:
- meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3] level 3 or higher
- meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [10], CWA 14167-3 [11] or CWA 14167-4 [12]
- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [13] or equivalent security criteria

The cryptographic device used to generate the CA Private Key meets the requirements in FIPS PUB 140-2 level 3.

c) 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.4.7

Subject key generation performed by the CA

d) CA Subject key generation SHALL be undertaken in a physically secured environment (see section 5.1), using a trusted system that can assure the secrecy of the Subject's Private Key.

Se 4.2 a) and 5.1

e) Subject keys generated by the CA MAY be software generated.

All Subject keys are generated by dedicated software, see 4.2 a)

f) After generation, software keys SHALL be stored in encrypted form, access protected with a secret Distribution Key. The Distribution Key SHALL either be:
- a random key generated by the CA
- a key chosen by the Subscriber/Subject and securely communicated to the CA

The key pair that is generated is stored in a PKCS#12 file, protected with a secret Distribution Key. The Distribution Key is derived from a randomly generated Activation Data which is stored encrypted until it is written to a blind impact printer.

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

Certificate Rekey require a new Certificate Application (see 4.1.2), however routine rekey is initiated automatically. Key/Certificate distribution is handled in the same way as for the initial key/Certificate distribution (see 4.2).

Subject key generation performed by the Subscriber

Support for Subscriber generated keys has not been implemented.

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

i) If the Private Key is for creating electronic signatures the Private Key SHALL be maintained under the Subject's sole control

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

k) Software keys SHALL be stored in encrypted form, access protected with secret Activation Data (see section 6.4.1)

l) Private Keys stored on token shall be access protected with secret Activation Data (see section 6.4.1)

6.1.2 Private Key delivery to entity

For CA generated private Subject keys the following requirements apply:

a) The Subject's Private Key SHALL be delivered to the Subject such that the secrecy and integrity of the key is not compromised.

The Private Key is sent from Buypass to the e-mail address provided by the Certificate Applicant as part of the Certificate Application. The Private Key is formatted as a PKCS#12 file and encrypted using a key derived from Activation Data (see 6.1.1 f). The Activation Data is distributed as described in 6.1.2 b).

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

The Activation Data is sent separate from the PKCS#12 file to the person identified as Subject Sponsor.

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

The Private Key is decrypted from the PKCS#12 file using the Activation Data sent to the Subject Sponsor.

When the Private Key is imported from the PKCS#12 file and onto the Subscriber system where it is to be used, the Subscriber, through the Subject Sponsor, is responsible for ensuring appropriate Private Key protection.

Buypass does not have any control with Subscribers' systems and their capabilities for Private Key protection once the Private Key is installed or made available to the target system. Buypass therefore explicitly, through the Subscriber Agreement, informs the Subscriber about its responsibility of applying appropriate Private Key protection.

d) Once delivered to the Subject, any copies of the Subject's Private Key held by the CA shall be destroyed.

Neither the Private Key nor the PKCS#12 file is stored by Buypass after they have been sent by e-mail to the Certificate Applicant.

6.1.3 Public Key delivery to Certificate issuer

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

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

Support for Subscriber generated keys has not been implemented.

6.1.4 CA Public Key delivery to users

The CA SHALL make the CA signature verification (public) keys available to Subjects and Relying Parties in a manner that assures the integrity of the CA Public Key and authenticates its origin.

The issuing CA and Root CA Certificate may be downloaded from the Buypass web (www.buypass.no).

6.1.5 Key sizes

CA keys

a) The selected key length and algorithm for CA signing key SHALL be one which is recognized by industry as being fit for the CA's signing purposes, see [9].

b) CA signature keys SHALL at least have a key size of RSA 2048.

Buypass CA signature keys for Class 2 Certificates are RSA 2048 bits.

CA signatures on Certificates, CRLs and OCSP responses are based on these keys and using SHA-1 or SHA-256 as hash algorithms.

Subject keys

c) Subject keys shall be generated using an algorithm and key length which are recognized by industry as being fit for the uses identified in this Certificate Policy during the validity time of the Certificate, see [9].

The Subject keys are RSA 2048 bits and generated within a cryptographic module meeting the requirements in FIPS 140-2 level 3.

6.1.6 Public Key parameter generation

No stipulations.

6.1.7 Parameter quality checking

No stipulations.

6.1.8 Hardware/software key generation

See 6.1.1

6.1.9 Key usage

CA keys
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.

Subject keys
Key usage combinations SHALL be set according to Buypass Class 2 Certificate and CRL profiles [5] and compliant with SEID prosjektet Anbefalte Sertifikatprofiler for personsertifikater og virksomhetssertifikater [4].

Buypass Class 2 Merchant Certificates comprise a single key pair/Certificate. The key pair/Certificate has key usage Digital Signature, Key encipherment and data encipherment and may be used for authentication and encryption purposes.

6.2 Private Key protection

6.2.1 Standards for cryptographic module

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 device which meets the requirements as defined in 6.1.1 b).

Each copy of the CA Private Key is kept within a cryptographic device that meets the requirements in 6.1.1 b). The only way for the Private Key to ever leave the cryptographic device is during CA key backup or CA key cloning see 6.2.4 b).

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.

All cryptographic devices containing the CA Private Key have access control mechanisms in place ensuring that the Private Key is not accessible outside the device. The only way the Private Key ever can leave the device is during Private Key backup or Private Key cloning as described in 6.2.4 b).

d) The CA SHALL ensure the security of the cryptographic device throughout its lifecycle. This includes protection against tampering.

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

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

All signing operations involving the CA Private Key are performed in Buypass' CA operations facility (see 5.1).

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. Private Key operations such as key generation and key backup require authentication by three Security Officers.

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.

Only personnel in trusted roles are able to access cryptographic devices. See also 6.2.1 c).

b) For backup purposes or cloning/redundancy purposes, the CA Private Key MAY be exchanged encrypted with another cryptographic device meeting the requirements in 6.1.1 b). This exchange is to take place using a trusted system in a physically secured environment (see section 5.1) and under the control of three (3) Security Officers.

During CA Private Key backup or CA Private Key Cloning, the Private Key is encrypted end-to-end during transit from one cryptographic device to another. This process takes place in the CA operations facilities and requires authentication of three Security Officers.

c) When outside the signature-creation device the CA private signing key SHALL be protected in a way that ensures the same level of protection as provided by the signature creation device.

See 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.

Cryptographic devices containing copies of the CA Private Key (whether for backup or archival) are protected under dual control. Mechanisms are in place that will ensure that unauthorized attempts to use either of these copies are detected.

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 have been archived will be kept in the archive until they are eventually destroyed.

6.2.6 Private Key entry into cryptographic module

See 6.1.1 and 6.2.4

The CA Private Key is generated within a cryptographic device. The CA Private Key is copied from the cryptographic device where the key was generated and onto other cryptographic devices to support either Private Key Backup or Private Key Cloning. Se 6.2.4 a).

6.2.7 Method of activating Private Key

CA Private Key

a) The Certificate signing keys SHALL only be activated and used within physically secure premises (see 5.1).

The CA Private Key is only activated and used within the CA operations facility. See also 6.2.1 d).

Subject Private Key

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

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

6.2.8 Method of deactivating Private Key

No stipulations.

6.2.9 Method of destroying Private Key

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

Buypass' routine for secure destruction of cryptographic devices containing a CA Private Key specifies that the device is shredded under dual control by two Security Officers. This routine is invoked whenever a cryptographic device is retired unless the device is required for archival.

No stipulations for Subject Private Keys.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulations.

6.3.2 Usage periods for the Public and Private Keys

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 end of their life cycle.

b) The use of the CA's private signing key SHALL be limited to that compatible with the hash algorithm, the signature algorithm and signature key length used when generating Certificates.

The CA Private Key has a lifetime as stated in the corresponding CA certificate. The lifetime of the CA Private Key depends on the size of the key and is set according to recommended practices. The algorithms used in conjunction with the signing key are chosen according to best practice for the given purpose. See also 4.7.

Subject keys

c) Subject Public Keys MAY be used to validate signatures made during the Certificate validity period after the validity period ends.

d) Subject Private Keys MUST NOT be used after the Certificate validity end time.

Subject key pairs generated before 18.03.2014 have a total lifetime of 3 years, and Subject key pairs generated later have a total lifetime of 5 years. Public Keys used for signature validation may be used after their corresponding Certificates have expired.

If major advances are made in the area of crypto analysis resulting in that the algorithms and key lengths used by Buypass for Subject keys (SHA-1 and/or SHA-256 and RSA 2048) no longer can be considered to give sufficient protection, Buypass may change the Subject key/Certificate lifetime or alternatively require stronger algorithms or longer keys.

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 (3) Security Officers.

CA Private Key Activation Data was randomly generated during the CA key ceremony and installed under the supervision of three Security Officers.

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

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

6.4.2 Activation Data protection

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

Access to CA Private Key Activation Data is protected under dual control and access requires participation from at least 1 Security Officer.

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

6.4.3 Other aspects of Activation Data

No stipulations.

6.5 Computer security controls

a) The CA SHALL implement Computer Security Controls according to best practice according to ISO/IEC 27002 [7] and in compliance with Buypass Information Security Policy [6].

Buypass' Information Security Management System (ISMS) has been certified against ISO/IEC 27001 where Buypass' Information Security Policy is a main component.

Buypass' ISMS is reasonably designed to:
a) comply with ISO 27002 as constrained by Buypass' statement of applicability
b) comply with the requirements defined by the WebTrust Program for Certification Authorities [21]
c) comply with the security requirements defined by the Normalized Certificate Policy (NCP) of ETSI TS 102 042 [8]
d) protect the confidentiality, integrity, and availability of:
(i) all Certificate Requests and data related thereto (whether obtained from Applicant or otherwise) in CA's possession or control or to which CA has access
(ii) the keys, software, processes, and procedures by which the CA verifies data, maintains a Repository, and revokes Class 2 Merchant Certificates
e) protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of the Data and Processes
f) protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Data or Processes
g) protect against accidental loss or destruction of, or damage to, any Data or Processes
h) comply with all other security requirements applicable to the CA by Norwegian law

Buypass' ISMS includes regular risk assessments that:
a) identify reasonably foreseeable internal and external threats 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 threats, taking into consideration the sensitivity of the Data and Processes
c) assess the sufficiency of the policies, 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 safeguards.

b) The Computer Security Controls SHALL conform to the requirements defined by the WebTrust Program for Certification Authorities [21] and to the Normalized Certificate Policy (NCP) requirements of ETSI TS 102 042 [8].

See 6.5 a)

6.6 Life cycle technical controls

a) The CA SHALL implement life cycle security controls according to best practice according to ISO/IEC 27002 [7] and in compliance with Buypass Information Security Policy [6].

Systems development and maintenance activities are designed to maintain CA system integrity. Strict control is maintained over access to program source libraries. Formal change control procedures exist and are followed for the implementation of software, scheduled software releases and emergency software fixes. See also 6.5 a).

b) The life cycle security controls SHALL conform to the requirements defined by the WebTrust Program for Certification Authorities [21] and to the Normalized Certificate Policy (NCP) requirements of ETSI TS 102 042 [8].

Se 6.5 a)

6.7 Network security controls

a) The CA SHALL implement network security controls according to best practice according to the Norwegian standard ISO/IEC 27002 [7] and in compliance with Buypass Information Security Policy [6].

See 6.5 a)

b) The network security controls SHALL conform to the requirements defined by the WebTrust Program for Certification Authorities [21] and to the NCP (Normalized Certificate Policy) requirements of ETSI TS 102 042 [8].

See 6.5 a)

6.8 Cryptographic module engineering controls

No stipulations.

See 6.1.1 b)

7 Certificate and CRL profiles

The Certificate and CRL profiles SHALL be described in Buypass Class 2 Certificate and CRL profiles [5] and the document SHALL be made publicly available on the Buypass web (www.buypass.no).

Certificate profiles SHALL be in accordance with the SEID profile for Certificates issued to organizations [4].

The OCSP profile SHALL conform to the specifications contained in RFC 2560 [15].

8 Specification administration

8.1 Specification change procedures

Buypass Policy Board MAY amend the Certificate Policy for Buypass Class 2 Merchant Certificates [14] or the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] at its own discretion.

8.2 Publication and notification procedures

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

Buypass MAY change any part of the Certificate Policy for Buypass Class 2 Merchant Certificates [14] or the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] with 90 days advance notice.

If Buypass deems a change not to be of material significance for the majority of Subscribers and Relying Parties, the change MAY be implemented subject to 30 days advance notice.

Any change that may materially influence users of the Certificate Policy for Buypass Class 2 Merchant Certificates [14] or the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] SHALL be published on the Buypass web (www.buypass.no).

Users that are influenced by a change MAY comment upon it. Whether or not comments are honored, SHALL solely be for Buypass Policy Board to decide. A change in the Certificate Policy for Buypass Class 2 Merchant Certificates [14] or the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] that is amended SHALL be subject to a new advance notice.

Modifications to either the Certificate Policy for Buypass Class 2 Merchant Certificates [14] or the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] 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 the Buypass web (www.buypass.no).

In the event that Buypass makes a significant modification to either the Certificate Policy for Buypass Class 2 Merchant Certificates [14] or the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] the respective document version number will be updated accordingly. In this case a change notification will be published on the Buypass web either 90 or 30 days before the new document version becomes effective. 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 Class 2 Merchant 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.

8.3 CPS approval procedures

No stipulations.

The Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] has been approved by Buypass Policy Board. All document changes have to be formally approved by Buypass Policy Board.