CERTIFICATE PRACTICE STATEMENT

BUYPASS CLASS 3 SSL CERTIFICATES

Effective date: 11.11.2008

PUBLIC

Version: 1.0
Document date: 11.11.2008

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

History of change

Version	Date	Status	Description/Change
1.0	07.11.2008	Approved	Approved by the Policy Board

Table of content

DEFINITIONS

Terms	Definition
Activation Data	Data that gives access to the Private key
Authorised Subscriber Representative	A natural person who is either Subscriber, employed by the Subscriber, or an authorised agent 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.
Central Coordinating Register for Legal Entities (“Enhetsregisteret”)	Norwegian national register containing basic data (e.g. Organization name and Organization Number) about legal entities to coordinate information on business and industry that resides in various public registers 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 certification authority which issued it (see ITU-T Recommendation X.509)
Certificate Application	A Subscriber's application for an SSL Certificate.
Certificate Applicant	Authorised Subscriber Representative who has authority to submit a Certificate Application on behalf of the Subscriber. A Certificate Applicant fills the Certificate Requester role as defined by the CA/browser Forum [10].
Certificate Approver	Authorised Subscriber Representative who has authority to (i) act as a Certificate Applicant and to authorise other employees or third parties to act as a Certificate Applicant, and (ii) to approve Certificate Applications submitted by Certificate Applicants. A Certificate Approver fills the same role as defined by the CA/browser Forum [10].
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 Signing Request	An electronic request that contains the Subscriber's Public Key to which the Certificate is to be associated. In this document, a Certificate Signing Request denotes a PKCS#10 [14] formatted request that is submitted by a Subscriber as part of a Certificate Application.
Certificate Status Service	Revocation Status Service as defined in section 2.1.1.
Certification Authority	Authority trusted by one or more users to create and assign Certificates
Certification Practice Statement (CPS)	Statement of the practices which a Certification Authority employs in issuing Certificates (see [1])
Contract Signer	Authorised Subscriber Representative who has authority on behalf of Subscriber to sign Subscriber Agreements.
National Register of Business Enterprises (”Foretaksregisteret”)	National register for all Norwegian and foreign business enterprises in Norway.
Organization Number	Unique enterprise identification number as registered in the Norwegian Central Coordinating Register for Legal Entities.
Private Key	The key of a key pair that is kept secret by the holder of the key pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a key pair that MAY be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Terms	Definition
Relying Party	Recipient of a Certificate which acts in reliance on that Certificate (see [1])
Signing Authority	Authorization to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Subscriber.
Signing Authority Statement	A statement that expressly documents a person's Signing Authority.
SSL Authority	Authorization on behalf of the Subscriber to i. submit, and, if applicable, authorise a Certificate Applicant to submit, the SSL Certificate Application on behalf of Subscriber; ii. provide, and, if applicable, authorise a Certificate Applicant to provide, the information requested from Subscriber by the CA for issuance of the SSL Certificate; iii. approve SSL Certificate Applications submitted by a Certificate Applicant.
SSL Authority Statement	A Statement that expressly documents a person's SSL Authority.
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 Sponsor	A natural person appointed by the Subscriber to undertake the Subject's obligations under the Certificate Policy for Buypass Class 3 SSL Certificates [15].
Subscriber	Organization subscribing with a Certification Authority on behalf of one or more Subjects.
Subscriber Agreement	Contractual agreement or written statement that specifies all Subscriber obligations under the Certificate Policy for Buypass Class 3 SSL Certificates [15].

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 3 Certificate and CRL profiles
[6] ISO/IEC 27002:2005: Information technology - Security techniques . Code of Practice for Information Security Management.
[7] ETSI TS 102 042 - Policy requirements for certification authorities issuing public key Certificates - v.1.2.1 2005-05
[8] ETSI TS 102 176 - Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms - v.2.0.0 2007-07
[9] ISO/IEC 15408 (parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security".
[10] CA/Browser Forum, Guidelines for the Issuance and Management of Extended Validation Certificates, see http://www.cabforum.org for current version.
[11] AICPA/CICA, WebTrust Program for Certification Authorities, version 1.0, 25.august 2000.
[12] IETF RFC 2560 Internet X.509 PKI Online Certificate Status Protocol (OCSP), June 1999
[13] IETF RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002.
[14] IETF RFC 2586: PKCS #10: Certification Request Syntax Specification, Version 1.7, November 2000
[15] Certificate Policy for Buypass Class 3 SSL Certificates, version 0.9, July 2008
[16] This document
[17] 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)".
[18] 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)".
[19] 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".

1 Introduction

1.1 Overview

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

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

This document provides a Certification Practice Statement covering the following types of Class 3 SSL Certificates that are offered by Buypass:

1. Extended Validation (EV) SSL Certificates.
2. Standard SSL Certificates

Buypass is the Certification Authority (CA) for all Buypass Class 3 SSL Certificates.

A Subscriber denotes the organization that contracts with the CA for the issuance of SSL Certificates. For Key/Certificate management operations the Subscriber shall be represented by human persons in the role of Authorised Subscriber Representatives. The Subject denotes a non-human entity (web-server) that represents the Subscriber and which is the holder of the Private Key associated with the Public Key to which the Certificate is issued. The Subject shall be represented by a person in the role of a Subject Sponsor who undertakes the Subject’s obligations as defined in the Certificate Policy for Buypass Class 3 SSL Certificates [15].

An EV SSL Certificate Subscriber SHALL be either a Private Organization or a Government Entity according to the definitions in the CA/Browser Forum Guidelines [10]. All EV SSL Certificate Subscribers SHALL be registered in the Norwegian Central Coordinating Register for Legal Entities. Private Organizations SHALL additionally be registered in the Norwegian National Register of Business Enterprises.

A Standard SSL Certificate Subscriber SHALL be an organization that is registered in the Norwegian Central Coordinating Register for Legal Entities.

A Subject that is issued a Buypass Class 3 Certificate SHALL be a web-server that represents and is operated by, or on behalf of, the Subscriber.

The Certificate Policy for Buypass Class 3 SSL Certificates [15] and Certification Practice Statement for Buypass Class 3 SSL Certificates [16] conform to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates (“Guidelines”) published at http://www.cabforum.org. In the event of any inconsistency between the Certificate Practice Statement and those Guidelines, those Guidelines take precedence over this document.

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 3 SSL Certificates [15]. All Certificate Policy requirements contain either a SHALL, SHALL NOT, SHOULD, SHOULD NOT or MAY statement.
Text contained inside blue coloured text boxes are Certification Practice Statement related and specifies in more detail the practices employed by Buypass to meet the requirements of the Certificate Policy.

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

1.2 Identification

The Class 3 Certificate Policies covered by this document have been provided the following Certificate Policy Identifiers / OIDs;

- Certificate Policy for Buypass Class 3 Extended Validation (EV) SSL Certificates - OID 2.16.578.1.26.1.3.3
- Certificate Policy for Buypass Class 3 Standard SSL Certificates - OID 2.16.578.1.26.1.3.4

Relying Parties SHALL recognize a particular SSL Certificate as having been issued under one of the above policies by inspecting the Certificate Policies extension field of the Certificate, which then shall hold the respective policy OID above.

The same Buypass CA that is used to issue SSL Certificates also issues Certificates under the following Certificate Policies / OIDs:

- Certificate Policy for Buypass Class 3 Qualified Certificates - OID 2.16.578.1.26.1.3.1
- Certificate Policy for Buypass Class 3 Enterprise Certificates - OID 2.16.578.1.26.1.3.2

1.3 Community and Applicability

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

1.3.1 Applicability

Buypass Class 3 SSL Certificates are applicable for supporting

- authentication between web servers and web browsers
- web-based server-to-server authentication

Use of Buypass Class 3 SSL Certificates is restricted to web-based data communication conduits via TLS/SSL protocols. Any other use of Buypass Class 3 SSL Certificates is prohibited.

Primary Certificate Purposes

1. Identify the legal entity that controls a website: Provide a reasonable assurance to the user of an Internet browser that the website the user is accessing is controlled by a specific legal entity that is uniquely identified in the SSL Certificate; and
2. Enable encrypted communications with a website: Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

Secondary Certificate Purposes

The secondary purposes of an SSL Certificate are to help establish the legitimacy of a business claiming to operate a website and to provide a vehicle that can be used to assist in addressing problems related to phishing and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the owner of a website, SSL Certificates may help to:

1. Make it more difficult to mount phishing and other online identity fraud attacks using SSL Certificates;
2. Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves and their legitimate websites to users; and
3. Assist law enforcement in investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

Excluded Certificate Purposes

SSL Certificates focus only on the identity of the Subscriber named in the Certificate, and not on the behaviour of the Subscriber. As such, an SSL Certificate is not intended to provide any assurances, or otherwise represent or warrant:

1. That the Subscriber named in the SSL Certificate is actively engaged in doing business;
2. That the Subscriber named in the SSL Certificate complies with applicable laws;
3. That the Subscriber named in the SSL Certificate is trustworthy, honest, or reputable in its business dealings; or
4. That it is “safe” to do business with the Subscriber named in the SSL Certificate.

1.4 Contact Details

Buypass Policy Board is responsible for the Certificate Policy for Buypass Class 3 SSL Certificates [15] and Certification Practice Statement for Buypass Class 3 SSL Certificates [16] and their maintenance.

Contact point for questions regarding the Certificate Policy for Buypass Class 3 SSL Certificates [15] and Certification Practice Statement for Buypass Class 3 SSL Certificates [16] is:

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

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

Contact point for all other matters concerning Buypass Class 3 SSL Certificates is:

Buypass Kundeservice
Serviceboks
N-2810 Gjøvik

Telephone: + 47 61 13 59 20
Fax: + 47 61 13 58 50
Email: kundeservice@buypass.no

2 General Provisions

2.1 Obligations

Buypass operates as both the CA and RA for all Certificates issued under the Certificate Policy for Buypass Class 3 SSL Certificates [15] and thereby fulfills all CA and RA obligations in this section.

2.1.1 CA obligations

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

- Registration service
- Certificate generation service
- Dissemination service
- Revocation management service
- Revocation status service

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

None of the CA/RA services are subcontracted by Buypass

The CA SHALL be responsible for providing its CA/RA services in conformance with the Certificate Policy for Buypass Class 3 SSL Certificates [15] and consistent with the Certification Practice

Statement for Buypass Class 3 SSL Certificates [16], even when functionality is undertaken by sub-contractors.

The CA SHALL warrant that the identity of the Subscriber that appears in an issued SSL Certificate is accurate and correct at the time of issuance.

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

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

The CA SHALL warrant that Subscriber named in the SSL Certificate has the exclusive right to use the domain name(s) listed in the SSL Certificate.

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

The CA SHALL maintain data security through development, implementation, and maintenance of a comprehensive Security Program that comply with the requirements of the CA/Browser Forum Guidelines [10].

2.1.2 RA obligations

An RA operating under the Certificate Policy for Buypass Class 3 SSL Certificates [15] SHALL;

a) receive SSL Certificate Applications from Subscribers, both initial applications (see 4.1.1) and rekey applications (see 4.1.2).
b) verify all information submitted by Subscribers, both for initial applications and for rekey applications and if such verification is successful, submit a request to the CA for the issuance of a Buypass Class 3 SSL Certificate .
c) receive and verify requests from Subscribers for the revocation of Buypass Class 3 SSL Certificates, and if the verification of a revocation request is successful, submit a request to the CA for the revocation of such Buypass Class 3 SSL Certificate
d) notify Subscribers that a Buypass Class 3 SSL Certificate has been issued to them.
e) notify Subscribers that a Buypass Class 3 SSL Certificate issued to them has been revoked or will soon expire.

2.1.3 Subscriber Obligations

The Subscriber SHALL ensure that all obligations of the Subscriber Agreement are fulfilled. As minimum:

a) The Subscriber SHALL submit accurate and complete information to the RA in accordance with the requirements in the Certificate Practice Statement for Buypass Class 3 SSL Certificates [16].

b) The Subscriber SHALL maintain correct Subscriber information, and notify the RA or CA of any changes to this information.

c) The Subscriber SHALL request the Certificate to be revoked when a valid revocation reason exists (see 4.4.1).

d) In case of SSL Authority pre-authorisation (see 3.1.2 e), the Subscriber SHALL inform the RA or CA whenever a pre-authorised Subscriber Representative no longer is authorised to represent the Subscriber.

e) The Subscriber SHALL be responsible for ensuring that restrictions on Private Keys and Certificates use are maintained.

f) The Subscriber SHALL install the SSL Certificate only on the server accessible at the domain name listed in the SSL Certificate.

g) The Subscriber SHALL generate a new, secure, and cryptographically sound Key Pair to be used in association with the Subscriber's SSL Certificate and SSL Certificate Application.

h) Reasonable care SHALL be exercised to avoid unauthorised use of the Subjects Private Keys.

i) The Subscriber SHALL NOT install or use the SSL Certificate(s) until it has been reviewed and the accuracy of the data in each SSL Certificate has been verified.

j) In the case of being informed that the CA has been compromised, the Subscriber SHALL ensure that the Private Key is no longer used by the Subject.

k) The Subscriber SHALL inform the Subject Sponsor(s) 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 provisioning of services (see 2.1.1) involves subcontracting, outsourcing or other third party arrangements. If the subcontractor agreement involve or relate to the issuance or maintenance of EV SSL Certificates, the agreement SHALL include (directly or by reference) the applicable requirements of the CA/Browser Forum Guidelines [10]

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

No subcontractors used by Buypass are involved in the issuance or maintenance of Buypass Class 3 SSL Certificates.

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 3 SSL Certificates [15].

The Relying party SHALL

- restrict reliance on Buypass Class 3 SSL Certificates to the purposes for those Certificates as defined by the Certificate Policy for Buypass Class 3 SSL Certificates [15].
- acknowledge applicable liability caps and warranties as defined by the Certificate Policy for Buypass Class 3 SSL Certificates [15].
- read and agree to all terms and conditions of the Buypass Class 3 SSL Certificate Policy and the Relying Party Agreement
- rely on a Buypass Class 3 SSL Certificate only if such reliance is reasonable in the circumstances, including determining whether such reliance is reasonable given the nature of the security and trust provided by a Buypass Class 3 SSL Certificate and the value of any transaction that may involve the use of a Buypass Class 3 SSL Certificate
- consult the most recent revocation status information in order to establish whether any of the Certificates in the certification path have been revoked.
- verify Buypass Class 3 SSL Certificates, including use of revocation services, in accordance with best practice certification path validation as defined by RFC 3280 [13].

If it is not possible to perform all of the above, the Relying Party shall not trust and make use of the Certificate.

2.2 Liability

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

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

- **For Buypass Class 3 Extended Validation (EV) SSL Certificates:** 2.000 USD (two thousand United States Dollars) per Subscriber or Relying Party concerning a specific Certificate or any services provided in respect to this Certificate.

- **For Buypass Class 3 Standard SSL Certificates:** The total liability for all damages sustained by all Subscribers and Relying Parties concerning a specific Certificate or any services provided in respect to this Certificate is limited in the aggregate to 100.000 USD (one hundred thousand United States Dollars).

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

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

Buypass has implemented the defined limitations of liability in its Subscriber Agreements and Relying Party Agreements.

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

Buypass maintains insurances to protect its Class 3 SSL service offering that complies with the requirements of the CA/Browser Forum Guidelines [10].

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

Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers SHALL indemnify and hold Buypass harmless from and against any and all liabilities, losses, costs, expenses, damages, claims and settlement amounts arising out of or relating to any reliance by a Relying Party on any Buypass Class 3 SSL Certificate or any service provided in respect to Buypass Class 3 SSL 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 unauthorised use of the Subscriber's Private Key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) 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 3 SSL Certificate or any service provided in respect to Buypass Class 3 SSL 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 and/or Relying Party Agreement MAY include additional indemnity obligations.

2.3.2 Fiduciary relationships

Issuance of Certificates in accordance with the Certificate Policy for Buypass Class 3 SSL Certificates [15] 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 and Relying Party 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 3 SSL Certificates [15], the Certification Practice Statement for Buypass Class 3 SSL Certificates [16], all related Subscriber Agreements and all related Relying Party Agreements.

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

2.4.2 Severability, Survival, Merger, Notice

Severability
In the event that a clause or provision of the Certificate Policy for Buypass Class 3 SSL Certificates [15] or the Certification Practice Statement for Buypass Class 3 SSL Certificates [16] 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 SSL Certificates issued for the remainder of the validity periods of such Certificates, also upon termination or expiration of the Certificate Policy for Buypass Class 3 SSL Certificates [15], the Certification Practice Statement for Buypass Class 3 SSL Certificates [16], any Subscription Agreements and any Relying Party Agreements.

Merger
The Rights and Obligations of Buypass as CA/RA MAY be modified only in a writing signed or authenticated by a duly authorised 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 3 SSL Certificates [15], the Certification Practice Statement for Buypass Class 3 SSL Certificates [16], a Subscription Agreement, or a Relying Party 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 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 3 SSL Certificate or any services provided in respect to any Buypass Class 3 SSL Certificate that is not resolved by alternative dispute resolution SHALL be brought to a Norwegian court for settlement. Oslo District Court shall be the exclusive first instance venue for all such disputes.

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

2.5 Fees

The fees for services provided by Buypass in respect to Buypass Class 3 SSL Certificates SHALL be published on the Buypass web http://www.buypass.no. These fees are subject to change, and any such changes SHALL become effective immediately after they have been published.

The service fees charged by Buypass for Buypass Class 3 SSL Certificates are published under http://www.buypass.no/

2.6 Publication and Repositories

The Certificate Policy for Buypass Class 3 SSL Certificates [15], the Certification Practice Statement for Buypass Class 3 SSL Certificates [16] SHALL be publicly available on the Buypass web (http://www.buypass.no) 24x7.

The Certificate Policy for Buypass Class 3 SSL Certificates [15] and the Certification Practice Statement for Buypass Class 3 SSL Certificates [16] are published on the Buypass web (http://www.buypass.no).

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

Every Class 3 SSL Certificate issued by Buypass contains a *CRL distribution point* Certificate extension that contains a URL for CRL retrieval (http://crl.prod.buypass.no/crl/BPClass3CA1.crl) and an *Authority Information Access* Certificate extension that contains a URL for OCSP service access (https://ocsp.prod.buypass.no/BPClass23). Both revocation status services are available 24x7.

2.7 Compliance Audit

a) The CA SHALL be audited once per calendar year for compliance with the practices and procedures set forth in the Certification Practice Statement for Buypass Class 3 SSL Certificates [16].

Buypass has already undergone, and will continue to undergo at least once per calendar year, an independent audit by a licensed WebTrust auditor against;
(i) the WebTrust Program for CAs
(ii) the WebTrust EV Program

As a result, Buypass has received, and will continue to maintain, a WebTrust Seal of Assurance for CAs as well as an authorisation to issue EV SSL Certificates.

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

The results of the most recent compliance audit is posted on the Buypass web (http://www.buypass.no).

b) The compliance audit SHALL be performed by a Buypass independent and certified public accounting firm.

Buypass uses a licensed WebTrust auditor for all WebTrust Program audits.

c) The CA SHALL perform ongoing self audits against a randomly selected sample of at least three percent (3%) of the EV SSL Certificates issued.

Buypass has a routine for this that is regularly conducted by a Security Auditor.

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/private;
- Certificates
- Certificate revocation status information

All other information about Subscribers, Subscriber Representatives and their use of Buypass services will be treated as confidential/private by Buypass.

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 3 SSL 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 an SSL Certificate, which information SHALL remain the property of the Subscriber. Buypass and Subscribers SHALL grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the applicable Relying Party Agreement.

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

d) Buypass SHALL retain all Intellectual Property Rights in and to the Certificate Policy for Buypass Class 3 SSL Certificates [15], the Certification Practice Statement for Buypass Class 3 SSL Certificates [16].

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Identification/Authentication of Subscriber and Subscriber Representatives

a) The following Subscriber information SHALL be obtained by the RA during initial registration:
   1. Full name and legal status of the Subscriber as defined in the Norwegian Central Coordinating Register for Legal Entities.
   2. The Subscribers' Organization Number as defined in the Norwegian Central Coordinating Register for Legal Entities.
   3. The Subscriber's domain name(s) to be included in the Certificate
   4. The address of Subscriber's Place of Business including street and building number, postal code (zip code), city, country and main telephone number.
   5. Name and contact information of all Subscriber Representatives authorised to operate as either Certificate Applicant, Certificate Approver or Contract Signer.

As part of an initial "Subscriber Registration and Subscriber Agreement Signing" step (see 4.1.1) the Subscriber will register the following information with Buypass using a web based registration procedure:

- The Subscriber's Organization Name and Organization Number as registered in the Norwegian Central Coordinating Register for Legal Entities.
- The address of Subscriber's Place of Business including street and building number, postal code (zip code), city, country and main telephone number.
- Domain name(s) either owned by or controlled by the Subscriber that the Subscriber wants SSL Certificates issued to.
- Name, Social Security Number and contact information for the responsible Contract Signer.
- Name, Social Security Number and contact information of Certificate Applicants and/or Certificate Approvers if there are Subscriber Representatives other than the Contract Signer that are authorised be able to operate in these roles.

All information registered is incorporated into a Subscriber Agreement that is signed and thereby confirmed by the Contract Signer. If the Subscriber later on wants to add, remove or change registered Subscriber information, the Subscriber needs to go through a new "Subscriber Registration and Subscriber Agreement Signing" step (see 4.1.1). An exception is the following changes that may be performed without going through a new "Subscriber Registration and Subscriber Agreement Signing" step:

- Certificate Approvers may change information about domain name(s) either owned by or controlled by the Subscriber that the Subscriber wants SSL Certificates issued to.
- The Contract Signer and Certificate Approvers may change information about authorised Certificate Applicants.

b) 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 Authorisation of Subscriber Representatives

The RA SHALL be able to identify Certificate Applicants, Certificate Approvers and Contract Signers as Authorised Subscriber Representatives;

- The Subscriber MAY authorise a single person to fill one, two, or all three of these roles.
- The Subscriber MAY authorise more than one person to fill each of these roles.
- An authorised Contract Signer is by definition also an authorised Certificate Approver.
- An authorised Certificate Approver is by definition also an authorised Certificate Applicant.

a) A Contract Signer's **Signing Authority** SHALL be established through a **Signing Authority Statement**. Accepted Signing Authority Statements MAY be;
   - Information obtained from the Norwegian National Register of Business Enterprises or the Norwegian Central Coordinating Register for Legal Entities identifying the Contract Signer as a person that is entitled to bind the Subscriber organization by signature.
   - Independent Confirmation from Subscriber as defined by [10].
   - Accountant Letter as defined by [10].
   - Legal Opinion as defined by [10].
   - Corporate Resolution as defined by [10].

Buypass initially consults the National Register of Business Enterprises / Central Coordinating Register for Legal Entities directly to verify whether the identified Contract Signer is registered as a person that is entitled to bind the Subscriber organization by signature or by procurationem.

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

b) A Certificate Approver's **SSL Authority** SHALL be established through an **SSL Authority Statement.** Accepted SSL Authority Statements MAY be;
   - Statements of Signing Authority as defined in a).
   - Independent Confirmation from a Contract Signer in compliance with the requirements of [10].
   - Independent Confirmation as defined by [10].
   - Accountant Letter as defined by [10].
   - Legal Opinion as defined by [10].
   - Corporate Resolution as defined by [10].

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

c) A Certificate Applicant's **authority to submit and sign an SSL Certificate Application** SHALL be established through;
   - Statements of Signing Authority or EV Authority as defined in a) and b) respectively.
   - an express authorisation statement issued by an authorised Certificate Approver or Contract Signer.

The Contract Signer may explicitly authorise one or several Certificate Applicants through the Subscriber Agreement that is signed (either initial agreement or later amendments). Buypass verifies the authenticity of the authorisation by contacting the Contract Signer.

Buypass also accepts express authorisation statements from already authorised Certificate Approvers. Buypass verifies the authenticity of such authorisation statements by contacting the Certificate Approver.

d) SSL Authority Statements / Signing Authority Statements SHALL be verified according section 4.1.1.

See 4.1.1.

e) The CA and Subscriber MAY enter into a written agreement, signed by a Contract Signer on behalf of Subscriber, whereby, for a specified term, Subscriber expressly authorises one or more Certificate Approver(s) designated in such agreement to exercise SSL Authority with respect to each future Certificate Application submitted on behalf of Subscriber. The CA/Browser Forum Guidelines [10] defines further requirements in this case.

As part of the Subscriber Registration process (see 4.1.1), the Subscriber enters into a Subscriber Agreement with Buypass. This Subscriber Agreement, signed by the Contract Signer, may expressly authorise one or several Certificate Approver(s) to exercise SSL Authority with respect to each future Certificate Application submitted on behalf of Subscriber. In this case, the Subscriber Agreement provides that the Subscriber is obligated under the Subscriber Agreement for all Certificate Applications issued by or approved by these Certificate Approvers until such SSL Authority is revoked.

3.2 Routine Rekey

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

Subscriber information and authorisations 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 routine rekey, the statements in 3.1.1 applies.

3.3 Rekey after Revocation

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

See 3.2.

3.4 Revocation Requests

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

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

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

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

See 4.4.3 b)

4 Operational Requirements

4.1 Certificate Application

4.1.1 Initial Application

The application procedure consists of the following main steps;

a) **Subscriber Registration and Subscriber Agreement Signing:** The Subscriber registers with Buypass Subscriber information as defined in section 3.1.1 as well as proof of authorisation for Certificate Applicants, Certificate Approvers and Contract Signers as described in 3.1.2. The Subscriber also provides to Buypass a Subscriber Agreement signed by the authorised Contract Signer.

b) **Certificate Application including Certificate Signing Request Submission:** A Certificate Applicant identified and authorised as part of Subscriber Registration provides to Buypass Certificate Application, including a PKCS#10 Certificate Signing Request. For EV SSL Certificate Applications in particular, the Certificate Applicant signs the Certificate Application.

c) **Certificate Application Approval:** An authorised Certificate Approver explicitly approves the Certificate Application (not needed if the Certificate Applicant in b) is also an authorised Certificate Approver).

a) The Certificate Applicant, Certificate Approver and Contract Signer SHALL register with an RA as Authorised Subscriber Representatives either prior to, or at the time of, applying for a Certificate. Section 3.1 defines necessary requirements for identification, authentication and authorisation.

The persons authorised by a Subscriber to exercise the Contract Signer, Certificate Approver and Certificate Applicant roles are registered either before or at the time the Subscriber applies for a particular Certificate. See section 3.1 regarding identification, authentication and authorisation.

b) The Subscriber SHALL provide to the RA:
   i. All Subscriber information as defined in section 3.1.
   ii. A Certificate Application signed by a Certificate Applicant.
   iii. A legally enforceable Subscriber Agreement signed by a Contract Signer that specifies the rights and responsibilities of the parties.

Submission of required Subscriber information as well as a signed Subscriber Agreement is performed during the "Subscriber Registration and Subscriber Agreement Signing**"** step described in the beginning of section 4.1.1. Certificate Application submission relates to the "Certificate Application including Certificate Signing Request Submission**"** step in the beginning section 4.1.1.

c) For EV Certificates, the contents of the Subscriber Agreement SHALL comply with the requirements of the CA/Browser Forum Guidelines [10].

The Subscriber Agreement for all Class 3 Certificates complies with the applicable requirements defined by the CA/Browser Forum Guidelines [10].

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

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

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

Buypass does not use external RAs.

f) The controls and procedures used to verify the Certificate Application SHALL conform to the information verification requirements defined by the CA/Browser Forum Guidelines [10] and SHALL establish:
   i. that the Certificate Application is accurate and complete.
   ii. that the Subscriber is registered in the Norwegian Central Coordinating Register for Legal Entities and the National Register of Business Enterprises (Private Organizations only) and that Subscriber information registered conform with information provided in the Certificate Application (see section 3.1.1).
   iii. that the Certificate Applicant, Certificate Approver and Contract Signer are Authorised Subscriber Representatives according to the requirements described in section 3.1.2.
   iv. that the Contract Signer has signed the Subscriber Agreement.
   v. that the Certificate Applicant has signed the Certificate Application (for EV Certificates only).
   vi. that the Subscriber is a registered holder or has exclusive control of the domain name to be included in the SSL Certificate.

For each Certificate Application processed, Buypass use established controls to ensure that:
- all mandatory Subscriber information (see 3.1.1) has been obtained from the Subscriber.
- the Subscriber's Organization Name and Organization Number exist in the National Register of Business Enterprises and/or the Norwegian Central Coordinating Register for Legal Entities.
- authorisation has been established for all registered Certificate Applicant(s), Certificate Approver(s), Contract Signer(s) as required by their respective role, see section 3.1.2.
- for each domain name registered by the Subscriber, that the Subscriber is either the registered holder of that domain or has exclusive control over that domain.
- a registered and authorised Contract Signer has signed the Subscriber Agreement.
- for EV Certificate Applications specifically, that a registered Certificate Applicant has signed the Certificate Application.

Each of the above controls is performed according to verification methods that have been defined as acceptable by the CA/Browser Forum Guidelines [10].

Each of the defined controls involves a specific set of Subscriber related information elements. Specific information elements as required by the CA/Browser Forum Guidelines [10] are tagged with a 1 year validity period at the point in time when the information element has been successfully verified by Buypass. In order for a Certificate Application to be accepted by Buypass (see "Certificate Application including Certificate Signing Request Submission" step in section 4.1.1), all Subscriber information registered by Buypass through the initial "Subscriber Registration and Subscriber Agreement Signing" step (see section 4.1.1) or later Subscriber information changes (see section 3.1.1) need to still be valid. If any of the required information elements has expired, the Subscriber is forced to go through the "Subscriber Registration and Subscriber Agreement Signing" step again.

Certificate issuance (see 4.2) will only take place after all information items has been successfully verified through the defined controls.

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

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

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

h) Auditable controls SHALL be in place to ensure separation of duties such that no person single-handedly can both validate and authorise the issuance of an SSL Certificate.

Buypass personnel involved in validation and authorisation of Certificate Applications have either one of two roles (no person will assume both roles);
A) Validator role; responsible for information gathering and initial information validation.
B) Authoriser role; responsible for a second independent examination and validation of all information gathered.
Personnel in both roles have to approve the Certificate Application before authorisation is given to issue the SSL Certificate.

i) Rejected Certificate Applications due to suspected phishing or other fraudulent usage or concerns SHALL be recorded in an internally managed database used to flag suspicious Certificate Applications.

Buypass records every rejected Certificate Application in an internal Buypass controlled database. Every time a new Certificate Application is received, this database is consulted in order to identify potential suspicious Certificate Applications.

j) All Certificate Application data, including the Subscriber's Authorisation Statements (see 3.1.2), SHALL be retained and archived.

All Certificate Application data, both electronic and paper based, are retained and archived according to section 4.6.

4.1.2 Rekey application

The requirements in section 4.1.1 SHALL apply also to a rekey application, whether the Certificate Application involves a routine rekey or a rekey after revocation.

Buypass will contact the Subscriber by e-mail or by phone with information that an existing Certificate is about to expire at the latest one month before the Certificate's expiry date.

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

Certificate renewal is not supported.

4.2 Certificate Issuance

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

Buypass confirms all Certificate Applications by contacting an authorised Certificate Approver. The Certificate Approver is registered as part of the initial Subscriber Registration procedure, see 4.1.1.

b) The CA SHALL ensure that the Subscriber has possession of the Private Key associated with the Public Key presented for certification.

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

c) If Private Key proof of possession validation fails during CAs verification of a Certificate Signing Request, the Certificate SHALL NOT be issued and the Certificate Applicant SHALL be notified without undue delay.

If Certificate Signing Request signature verification fails, the Certificate Application rejected and the Certificate Applicant is notified without undue delay.

d) All SSL Certificates that are issued SHALL follow the Certificate profile requirements defined in section 7.

All Class 3 SSL Certificates that are issued (both EV SSL Certificates and Standard SSL Certificates) follow the Certificate profiles as documented in section 7.

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

Every SSL Certificate that is issued is distributed to the Subscriber by attaching it to an e-mail that is sent to the Certificate Applicant.

Relying Parties will obtain a particular Subscriber Certificate through the SSL/TLS session for which that Certificate is used.

f) When the CA detects duplicate Public Keys, the Certificate Application SHALL be rejected.

Buypass records in an internal database all public keys that are received through Certificate Applications. Whenever a public key is received for which a duplicate already exists in the database, the Certificate Application is rejected.

g) The validity period for an EV Certificate SHALL NOT exceed twenty seven months. If the validity period exceeds twelve months, the CA SHALL revalidate Subscriber information every twelve months for as long as the Certificate is still valid, see [10].

Buypass EV SSL Certificates will have a default lifetime of 1 year (12 months).

All recorded Subscriber information is revalidated before the information is one year old.

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

Every time a new SSL Certificate has been issued for a Subscriber, Buypass sends a notification e-mail to both the Certificate Applicant and to the Certificate Approver that were involved when the Certificate was issued.

4.3 Certificate Acceptance

a) The Subscriber SHALL review and verify the accuracy of the data in each SSL Certificate that it receives.

The e-mail that is sent to the Subscriber that contains the issued SSL Certificate (see 4.2 e) will include a description, or a link to how such a description may be obtained, of how the Subscriber can verify relevant information parameters in the Certificate.

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 a notification within this 2 weeks verification period, Buypass assumes that the Certificate, as it is made available, is accepted and deemed correct by the Subscriber.

4.4 Certificate Suspension and Revocation

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

a) The CA SHALL offer a revocation management service that can accept and respond to revocation requests and related inquiries on a continuous 24x7 basis.

Buypass offers a 24x7 revocation service where Subscribers can submit revocation requests either by phone or through web (http:\\www.buypass.no).

Buypass also offers a 24x7 problem reporting service where Subscribers, Relying Parties and other third parties can report complaints or suspected Private Key compromise, EV SSL Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV SSL Certificates. The problem reporting service is also available by phone or through web (http:\\www.buypass.no). Buypass will acknowledge receipt of every report immediately and begin further investigations within 24 hours to decide whether revocation or other appropriate action is warranted. All problem reports are handled in compliance with the requirements of the CA/Browser Forum Guidelines [10].

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

The revocation 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 request is denied, 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/revocation is available immediately after the Certificate has been suspended/ 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, i.e. within 12 hours after the Certificate was suspended/revoked.

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

Buypass offers revocation status information 24 hours per day, 7 days per week. Revocation status information is offered both as a CRL service and as an OCSP service.

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

Service information that is considered relevant for Subscribers and/or Relying Parties are put out on the Buypass web. Subscribers and Relying Parties may subscribe to a direct notification service.

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 SSL 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 suspended or revoked.

The registered Certificate Applicant and the Certificate Approver for a specific SSL Certificate is notified by e-mail once the Certificate has been either suspended or revoked.

4.4.1 Circumstances for revocation

A Certificate SHALL be revoked if:

a) The Subscriber requests revocation of its SSL Certificate;
b) The Subscriber indicates that the original Certificate Application was not authorised and does not retroactively grant authorisation;
c) The CA obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the SSL Certificate) has been compromised, or that the Certificate has otherwise been misused;
d) The Subscriber terminates it's use of the Subject Private Key while the corresponding Public Key Certificate is still valid.
e) The CA receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
f) The CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the Certificate, or that the Subscriber has failed to renew its domain name;
g) The CA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
h) A determination, in the CA's sole discretion, that the Certificate was not issued in accordance with the terms and conditions of this Certificate Policy or, for EV Certificates in particular, the CA/Browser Forum Guidelines [10];
i) The CA determines that any of the information appearing in the Certificate is not accurate or correct.
j) The CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
k) The Certificate is an EV Certificate and the CA's right to issue EV Certificates under the CA/Browser Forum Guidelines [10] expires or is revoked or terminated, unless the CA makes arrangements to continue maintaining the CRL/OCSP Repository;
l) The Private Key of the CA's Root Certificate used for issuing that Certificate is suspected to have been compromised;
m) The CA receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the CA's jurisdiction of operation as described in the CA/Browser Forum Guidelines [10].
n) the Subscriber does not pay the service fees to Buypass (see section 2.5)
o) the Subscriber ceases to exist

4.4.2 Who can request revocation?

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

Certificate revocation may be requested by one of the Authorized Subscriber Representatives (Certificate Applicant, Certificate Approver or a Contract Signer) already registered with Buypass for that particular Subscriber and Certificate.

Buypass accepts Revocation Requests from previously unregistered Subscriber Representatives only if

(i) the revocation request is confirmed by an existing Certificate Applicant, Certificate Approver or Contract Signer, or
(ii) Buypass, through further investigation, has reason to beleive that a valid revocation reason exists (see 4.4.2 b).

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

Buypass is entitled to, and will request revocation of a Subscriber's SSL Certificate, at any time for any of the reasons set forth in section 4.4.1.

c) Revocation requests received from a non-authorised 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 Authorised Subscriber Representative, Buypass will make an effort to investigate whether there is a valid revocation reason.

4.4.3 Procedure for revocation request

a) Authorised 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, through web or by e-mail. Contact points for revocation are communicated to the Subscriber through the Subscriber Agreement and are available on Buypass' web site.

b) Revocation requests SHALL be authenticated and checked to be from an authorised source (see section 0). 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 that describe the different controls that need to be executed before the request is authorised and revocation is performed.

c) All previously revoked EV SSL Certificates and previously rejected EV SSL Certificate Requests due to suspected phishing or other fraudulent usage or concerns SHALL be recorded and the information SHALL be used to flag suspicious Certificate Applications.

All previously revoked EV SSL Certificates and previously rejected EV SSL Certificate Requests due to suspected phishing or other fraudulent usage or concerns is recorded. Every time a new Certificate Application is received, the recorded information is consulted in order to identify potential suspicious Certificate Applications.

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 Customer Service is directed to a standby service with authority to suspend the Certificate after reasonable assurance has been established that the request originates from an authorised 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 the HTTP protocol (URL=http://crl.prod.buypass.no/crl/BPClass3CA1.crl). The HTTP URL is included in the CRL Distribution Point extension of all SSL Certificates that are issued.

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. 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 SHALL check either the latest CRL or use the online Revocation status service (4.4.11) 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 (URL=https://ocsp.prod.buypass.no/BPClass23). The service URL is included in the AIA extension of all SSL Certificates that are issued.

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 whether 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 Subscriber'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 an SSL Certificate, including all information generated or received in connection with an SSL 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:
   i. CA key lifecycle management events, including:
      a) Key generation, backup, storage, recovery, archival, and destruction; and
      b) Cryptographic device lifecycle management events.
   ii. CA and Subscriber SSL Certificate lifecycle management events, including:
      a) SSL Certificate Applications, re-key applications and revocation;
      b) All verification activities required;
      c) Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
      d) Acceptance and rejection of SSL Certificate Applications;
      e) Issuance of SSL Certificates; and
      f) Generation of Certificate Revocation Lists (CRLs); and OCSP entries.
   iii. Security events, including:
      a) Successful and unsuccessful PKI system access attempts;
      b) PKI and security system actions performed;
      c) Security profile changes;
      d) System crashes, hardware failures, and other anomalies;
      e) Firewall and router activities; and
      f) Entries to and exits from the CA facility.

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

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

c) For each log entry, the the following elements SHALL be recorded.
   a) Date and time of entry;
   b) Identity of the person making the journal entry; and
   c) 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 unauthorised 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 unauthorised access to system resources are automatically processed every day against a predefined set of rules. Audit logs concerning physical access to Buypass operations facilities are regularly processed to ensure that all only authorised 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 few 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 off-site 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

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

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/RA services that Buypass is responsible for (see 2.1.1), then Buypass will, upon request, make archived audit records available to independent auditors as needed for the purpose of being used as evidence during legal proceedings.

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 authorisation.

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 authorisation. 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.

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 6.1.4).

The current Class 3 CA Certificate expires 9th. May 2015 and has a total lifetime of 10 years. A new CA key pair and a new CA Certificate will be generated at the latest 3 years before this date. During a transition period after a CA key changeover, both the old and the new CA will be operated in parallel.

Buypass may decide to perform key changeover earlier, especially if major advances is made in the area of crypto analysis resulting in that the algorithms and key lengths used by Buypass (SHA-1 and RSA 2048) no longer can be considered to give sufficient protection.

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 6.1.3.

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 enact in case of a disaster. The disaster recovery plan SHALL define;
   i. a disaster organization
   ii. 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
   iii. the recovery procedures used if computing resources, software and/or data are corrupted or suspected to be corrupted
   iv. how a secure environment is re-established
   v. 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/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.

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 incident/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. Physical security controls are in place to prevent non-authorised 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 or algorithm compromise the CA SHALL as a minimum provide the following undertakings:
   i. 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;
   ii. indicate that Certificates and revocation status information issued using this CA key may no longer be valid.

The disaster recovery plan, see 4.8, covers CA Key or algorithm compromise. The above undertakings are part of the supporting routines and procedures.

f) 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 following procedures SHALL be executed as a minimum:
   i. the CA SHALL inform the following of the termination: all Subscribers, Relying Parties and other entities with which the CA has agreements or other form of established relations. In addition, this information shall be made available to other Relying Parties;
   ii. the CA SHALL terminate all authorisation of subcontractors to act on behalf of the CA in the performance of any functions related to the process of issuing Certificates;
   iii. the CA SHALL perform necessary undertakings to transfer obligations for maintaining registration information, revocation status information and event log archives for their respective period of time as indicated to the Subscriber and Relying Party;
   iv. all copies of the CA private signing keys shall be destroyed or put beyond use.
   v. the revocation of unexpired unrevoked Subscriber Certificates, if required.

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

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

5 Physical, Procedural, and Personnel Security Controls

5.1 Physical Security Controls

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

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

Dual control has been implemented for physical access to the CA operations facilities. Access requires physical presence of two authorised 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 authorised person.

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

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

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

Buypass maintains procedures that cover secure and trusted asset handling, including transport of security sensitive assets off-site. Controls such as dual access and regular inventory control are designed to prevent and detect unauthorised 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:** controls that routines are complied with. The Security Auditor reads and maintains archives and audit logs
- **System Administrator:** is responsible for the operation of the system. The System Administrator is responsible for the installation of 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 in 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 a staffing of qualified personnel sufficient to maintain the required segregation of duties as well as the target service level. An overview of experience and qualifications for all personnel involved in CA/RA operations is maintained. Risk and vulnerability assessments that are performed regularly include an evaluation of personnel qualifications.

5.2.2 Number of 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 private CA keys ensure that the operations are witnessed by three persons assuming a Security Officer role.

b) Dual control is required to install and activate 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/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/RA facilities (see 5.1) as well as for logical access to CA/RA systems.

5.3 Personnel Security Controls

The CA SHALL ensure that personnel and employment/contractor practices 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 that persons assuming trusted roles have passed defined background checks and that they have gone through necessary education/training.

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

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

Thorough reference checks, including confirmation of previous employments and relevant education, are used prior to authorising 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 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.

Se 5.3.1 a)

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

Any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position will not be authorised 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 3 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 unauthorised actions

a) Appropriate disciplinary sanctions SHALL be applied to personnel violating the Certificate Policy for Buypass Class 3 SSL Certificates [15] 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 3 SSL Certificates [16] and supporting operational routines.

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

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

5.3.6 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/RA services as specified in section 2.1.1 are familiar with the Certificate Policy for Buypass Class 3 SSL Certificates [15] and the Certification Practice Statement for Buypass Class 3 SSL Certificates [16]. Both documents are available electronically.

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 authorised 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:
   i. meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3] level 3 or higher; or
   ii. meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [17], CWA 14167-3 [18] or CWA 14167-4 [19]; or
   iii. is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [9], or equivalent security criteria.

The cryptographic device used to generate the CA Private Key has been Common Criteria evaluated to EAL5. The device's Operating System has been evaluated according to ITSEC E6.

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 the Certificate Policy for Buypass Class 3 SSL Certificates [15].

See 4.7

Subject key generation performed by the Subscriber

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

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

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

6.1.2 Public key delivery to Certificate Issuer

The Public Key SHALL be delivered to the CA as part of a Certificate Signing Request. The Certificate Signing Request SHALL:
i. authenticate the Subscriber as the originator of the request
ii. contain proof that the Subscriber is in possession of the Private Key that corresponds to the Public Key in the request.

The Public Key is delivered by the Subscriber as part of a PKCS#10 formatted Certificate Signing Request. The signature on the request provides proof of possession of the Private Key. The authenticity of the request may be verified by forcing the Certificate Applicant to log in using electronic credentials issued by Buypass in order to submit the Certificate Application. Alternatively, manual verification may be used by contacting the Certificate Applicant.

6.1.3 CA public key delivery to users

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

The self-signed Class 3 CA Certificate is pre-installed in common World Wide Web browser and web server software by the applicable software manufacturers.

The CA Certificate may also be downloaded from Buypass through the following URLs;
Using LDAP: ldap://ldap.prod.buypass.no/dc=Buypass,dc=NO,CN=Buypass Class 3 CA 1
Using HTTP: http://www.buypass.no/Installasjoner/BP_Class_3_CA/Buypass_Class_3_CA_1.cer

The Certificate's SHA-1 Thumbprint is published on the Buypass web to enable Subscribers and Relying Parties to verify the Certificate's authenticity.

6.1.4 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 [8] and [10].

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

CA signatures on Certificates, CRLs and OCSP responses are generated using RSA 2048 and SHA-1.

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 [8].

d) For EV SSL Certificates, Certificates containing an RSA 1024 bit Subject key SHALL expire before 31 Dec 2010. After this date Subject keys SHALL have a minimum key size of RSA 2048 bits.

e) For Standard SSL Certificates, Certificates containing an RSA 1024 bit Subject key SHALL expire before 31 Dec 2011. After this date Subject keys SHALL have a minimum key size of RSA 2048 bits.

Currently, only RSA Subject keys are supported by Buypass. Upon reception of a Certificate Signing Request, Buypass will verify the key size used by the Subscriber. For EV Certificates, maximum Certificate lifetime is 2 years subject to the restrictions in d). For Standard SSL Certificates, the maximum Certificate lifetime is 3 years subject to the restrictions in e).

6.1.5 Public key parameter generation

No stipulations.

6.1.6 Parameter quality checking

No stipulations.

6.1.7 Hardware/software key generation

See 6.1.1.

6.1.8 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 [5] and compliant with [4].

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/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 / 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 is 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 that involve the CA Private Key is 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 requires authentication by three Security Officers.

6.2.3 Private key escrow

No stipulations.

Buypass do not use Private key escrow.

6.2.4 Private key backup

CA key backup

a) The CA private signing key SHALL be backed up, stored and recovered only by personnel in trusted roles.

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

b) For backup or cloning/redundancy purposes, the CA Private Key MAY be exchanged encrypted with another cryptographic device meeting the requirements in 6.1.1 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 / 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 is required to perform this backup process.

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.

Se 6.2.4 b)

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

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 unauthorised 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 has 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.

Subject Private Key

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

c) Dependent on support by the Subject, 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 completely destroyed under dual control 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.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

No stipulations.

Subscriber Certificates are archived by Buypass only until they expire.

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 total lifetime of 10 years, the same lifetime as the CA Certificate containing the corresponding Public Key. See also 4.7.

Subject keys

c) Subject private and Public Keys SHALL NOT be used beyond the Certificate validity period.

6.4 Activation Data

6.4.1 Activation Data generation and installation

a) CA Private Key Activation Data SHALL be generated by the CA using a random number generator and installed under the supervision of at least three (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 can not be easily guessed. The use of Activation Data 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 a 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 participation from 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 [6] and in compliance with Buypass Information Security Policy [9].

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 [11]
c) Comply with the security requirements defined by the Normalized Certificate Policy (NCP) of ETSI TS 102 042 [7].
d) Protect the confidentiality, integrity, and availability of: (i) all SSL Certificate Requests and data related thereto (whether obtained from Applicant or otherwise) in CA's possession or control or to which CA has access, and (ii) the keys, software, processes, and procedures by which the CA verifies e)Data, issues SSL Certificates, maintains a Repository, and revokes SSL Certificates;
e) Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of the Data and Processes;
f) Protect against unauthorised 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; and
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 unauthorised 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; and
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 [11] and to the Normalized Certificate Policy (NCP) requirements of ETSI TS 102 042 [7].

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 [6] and in compliance with Buypass Information Security Policy [9].

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 [11] and to the Normalized Certificate Policy (NCP) requirements of ETSI TS 102 042 [7].

See 6.5 a).

6.7 Network Security Controls

a) The CA SHALL implement Network Security Controls according to best practice according to ISO/IEC 27002 [6] and in compliance with Buypass Information Security Policy [9].

See 6.5 a).

b) The Network Security Controls SHALL be conform to the requirements defined by the WebTrust Program for Certification Authorities [11] and to the NCP (Normalized Certificate Policy) requirements of ETSI TS 102 042 [7].

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 [5] and the document SHALL be made publicly available at http://www.buypass.no.

The Certificate profile for Buypass Class 3 EV SSL Certificates SHALL conform to the current version of the CA/Browser Forum Guidelines [10].

The Certificate profile for all Buypass Class 3 SSL Certificates SHOULD conform to the SEID profile for Certificates issued to organizations [4].

The OCSP profile SHALL conform to the specifications contained in RFC 2560 [20].

8 Specification Administration

8.1 Specification Change Procedures

Buypass Policy Board MAY amend the Certificate Policy for Buypass Class 3 SSL Certificates [15] or the Certification Practice Statement for Buypass Class 3 SSL Certificates [16] 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 3 SSL Certificates [15] or the Certification Practice Statement for Buypass Class 3 SSL Certificates [16] 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 3 SSL Certificates [15] or the Certification Practice Statement for Buypass Class 3 SSL Certificates [16] SHALL be published on www.buypass.no.

Users that are influenced by a change MAY comment upon it. Whether or not comments are honoured, SHALL solely be for Buypass Policy Board to decide. A change to the Certificate Policy for Buypass Class 3 SSL Certificates [15] or the Certification Practice Statement for Buypass Class 3 SSL Certificates [16] that is amended SHALL be subject to a new advance notice.

Modifications to either the Certificate Policy for Buypass Class 3 SSL Certificates [15] or the Certification Practice Statement for Buypass Class 3 SSL Certificates [16] that in the judgement 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.

In the event that Buypass makes a significant modification to either the Certificate Policy for Buypass Class 3 SSL Certificates [15] or the Certification Practice Statement for Buypass Class 3 SSL Certificates [16] 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 3 SSL 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 3 SSL Certificates [16] has been approved by Buypass Policy Board. All document changes have to be formally approved by Buypass Policy Board.