Version: 5.3
Document date: 12.05.2022
Effective date: 12.05.2022

PUBLIC

Certification Practice Statement

Buypass ACME Certificates

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

www.buypass.no | 22 70 13 00

TABLE OF CONTENTS

1 Introduction

1.1 Overview

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

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

This document provides a Certificate Policy and a Certification Practice Statement covering the following categories of Buypass ACME Certificates that are offered by Buypass:

Buypass Go SSL Certificates

Buypass is the Certificate Authority (CA) for all Buypass ACME Certificates.

A Subscriber denotes the natural or legal person that contracts with the CA for the issuance of Buypass ACME Certificates. For Key/Certificate management operations the Subscriber shall be represented by natural persons in the roles of Authorized 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.

A Subject that is issued a Buypass ACME Certificate SHALL either be the Subscriber or a device under the control and operation of the Subscriber.

Buypass conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”) published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

1.1.1 CA hierarchy

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

The Buypass Class 2 CA hierarchy consists of the Buypass Class 2 Root CA and the three issuing CAs Buypass Class 2 CA 2, Buypass Class 2 CA 4 and Buypass Class 2 CA 5.

Buypass Class 2 CA 2 issues Buypass Class 2 SSL Certificates

Buypass Class 2 CA 4 issues (technically constrained) Buypass Organization Certificates.

Buypass Class 2 CA 5 issues Buypass Go SSL Certificates as specified in this document.

1.2 Document name and Identification

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

- Certificate Policy for Buypass Go SSL Certificates - OID 2.16.578.1.26.1.2.7

In addition, the Buypass ACME Certificates conforms to CA/Browser Forums Baseline Requirements and are assigned these CA/B Forum Certificate Policy Identifiers / OIDs:

- Buypass Go SSL Certificates - OID 2.23.140.1.2.1

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 one of the OIDs above.

1.2.1 Revisions

Version	Document Date	Description/Change
1.0	12.06.2017	Approved by Buypass Policy Board
2.0	04.08.2017	Included Certificate Authority Authorization (CAA)
2.1	05.01.2018	Included support for ECC, included CAA Errata, and included maximum certificate validity period of 825 days.
3.0	15.02.2018	Updated according to BR Self Assessment and included Certificate Transparency (CT) for all certificates.
4.0	31.05.2018	Converted to RFC 3647
4.1	12.09.2018	Changing domain validation methods, added Method 7.
4.2	19.10.2018	Change revocation and problem reporting to be compliant with BR Revocation Timeline Extension as specified in ballot SC6 v3.
4.3	18.10.2019	Changed procedures for CP/CPS notifications. Included information on ACME RFC 8555.
5.0	30.03.2020	Compliant with Mozilla Root Store Policy 2.7 ('No stipulation' etc). Included domain validation methods 17, 18 and 19 from BR.
5.1	01.10.2020	Changed domain validation methods, removed Method 10 and added Method 20. Changes in Audit logging procedures in section 5.4.
5.2	12.05.2021	Included methods to demonstrate private key compromise.
5.3	12.05.2022	General revision.

1.3 PKI Participants

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

1.3.1 Certification Authorities

Buypass is the Certificate Authority (CA) for all Buypass ACME Certificates.

1.3.2 Registration Authorities

Buypass is the Registration Authority (RA) for all Buypass ACME Certificates.

1.3.3 Subscribers

A Subscriber denotes the natural or legal person that contracts with the CA for the issuance of Buypass ACME Certificates.

1.3.4 Relying Parties

Relaying party is defined in section 1.6.1.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

Buypass ACME Certificates are applicable for supporting authenticating servers accessible through the internet.

Use of Buypass ACME Certificates is restricted to authenticating servers via TLS protocols. Any other use of Buypass ACME Certificates is prohibited.

1.4.1 Primary Certificate Purposes

1. Identify the website
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.

1.4.2 Secondary Certificate Purposes

The secondary purposes of a Buypass ACME Certificate are to provide a vehicle that can be used to assist in addressing problems related to phishing and other forms of online identity fraud.

1.4.3 Excluded Certificate Purposes

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

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

1.5 Policy administration

1.5.1 Organization Administering the Document

Buypass Policy Board is responsible for the Certificate Policy [18] and Certification Practice Statement [19] and their maintenance.

1.5.2 Contact Person

Contact point for questions regarding the Certificate Policy [18] and Certification Practice Statement Certificates [19] is:

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

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

For Problem Reporting use the online web service at https://www.buypass.com/ssl/support/ssl-problem-reporting or send an email to ca-security@buypass.no.

1.5.3 Person Determining CPS suitability for the policy

Refer to section 1.5.1.

1.5.4 CPS approval procedures

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

The Certification Practice Statement [19] are approved by Buypass Policy Board. All document changes must be formally approved by Buypass Policy Board.

1.6 Definitions and acronyms

1.6.1 Definitions

Terms	Definition
ACME client	An ACME compliant client supporting the client side operations of the ACME protocol.
Activation Data	Data that gives access to the Private Key
Authorization Domain Name	The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN

Terms	Definition
	returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.
Authorized Subscriber Representative	A natural person who is either Subscriber, employed by the Subscriber, or an authorized agent who has express authority to represent the Subscriber.
Base Domain Name	The portion of an applied-for FQDN that is the first domain name node left of a registry controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.
Automated Certificate Management Environment (ACME)	A communication protocol for automating interactions between Certificate Authorities and their users' web servers, allowing the automated deployment of Public Key infrastructure
Buypass	Buypass AS, registered in the Central Coordinating Register of Legal Entities (“Enhetsregisteret”) with organization number 983 163 327.
Buypass Policy Board	The Board responsible for all Certificate Policies in Buypass.
Buypass Web	Websites operated by Buypass, i.e. www.buypass.no and www.buypass.com.
Certificate Authority Authorization (CAA)	The CAA DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate misissue.
Certificate	An electronic document that uses a digital signature to bind a public key and an identity. In this document the term is used synonymously with Buypass ACME Certificate.
Certificate Application	A Subscriber's application for an SSL Certificate.
Certificate Applicant	Authorized Subscriber Representative who has authority to submit a Certificate Application on behalf of the Subscriber.
Certificate Authority (CA)	An organization that is responsible for the creation, issuance, revocation and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.
Certificate Policy (CP)	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
Certificate Rekey	The issuance of a new Certificate for a previously registered Subscriber based on a new key pair. This includes routine rekey, rekey prior to expiration and rekey after revocation.
Certificate Renewal	The issuance of a new Certificate for a previously registered Subscriber based on an existing Certificate without changing the Subscriber’s Public Key.

Terms	Definition
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 [13] formatted request that is submitted by a Subscriber as part of a Certificate Application.
Certificate Transparency (CT)	Certificate Transparency is Google's approach to mitigate the problem of misissued certificates by providing publicly auditable logs of all issued certificates (see [25]).
Certification Practice Statement (CPS)	Statement of the practices which a Certificate Authority employs in issuing Certificates (see [19])
Domain Contact	The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
Domain Name	The label assigned to a node in the Domain Name System.
Domain Name Registrant	Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or legal entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
Fully-Qualified Domain Name (FQDN)	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
Hardware Security Module (HSM)	A secure cryptographic module used to generate, store and handle cryptographic keys. The HSM provides logical and physical protection of the keys.
High Risk Request	A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.
High Security Zone	An area (physical or logical) protected by physical and logical controls that protects a CA's Private Key and cryptographic hardware.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.
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.

Terms	Definition
Public Key	The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Qualified Auditor	A natural person or legal entity that meets the requirements in Baseline Requirements. This includes an auditor accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403.
Relying Party	Recipient of a Certificate which acts in reliance on that Certificate (see [1])
Subcontractor	Party providing services on behalf of the CA.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subject Sponsor	A natural person appointed by the Subscriber to undertake the Subject's obligations under the Certificate Policy for Buypass ACME Certificates [18].
Subscriber	A natural person or legal entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement.
Subscriber Agreement	An agreement between the CA and the Subscriber that specifies the rights and responsibilities of the parties under the Certificate Policy for Buypass ACME Certificates [18].
Terms Of Service	See Subscriber Agreement.

1.6.2 References

[1] IETF RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework – 2003.
[2] FIPS PUB 140-1: "Security Requirements for Cryptographic Modules"
[3] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules"
[4] ETSI EN 319 412-4 – Certificate Profiles: Part 4: Certificate profile for web site certificates.
[5] Buypass Class 2 Certificate and CRL profiles, current version
[6] ISO/IEC 9594-8 Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
[7] ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
[8] ISO/IEC 27002:2013: Information technology - Security techniques. Code of Practice for Information Security Management
[9] ETSI TS 119 312 – Cryptographic Suites
[10] ISO/IEC 15408 (parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security"
[11] IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP), June 2014
[12] IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008
[13] IETF RFC 2586: PKCS #10: Certification Request Syntax Specification, Version 1.7, November 2000
[14] IETF RFC 8659: DNS Certification Authority Authorization (CAA) Resource Record, November 2019
[15] ETSI EN 319 401 – General policy requirements for Trust Service Providers
[16] ETSI EN 319 411-1 – Policy and security requirements for Trust Service Providers issuing certificates; Part 1 General requirements

[17] ETSI EN 319 411-2 – Policy and security requirements for Trust Service Providers issuing certificates; Part 2 Requirements for Trust Service Providers issuing EU Qualified Certificates
[18] Certificate Policy for Buypass ACME Certificates, included in Certification Practice Statement for Buypass ACME Certificates [19]
[19] Certification Practice Statement for Buypass ACME Certificates, this document
[20] Policy for sikkerhet og kvalitet i Buypass
[21] CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, see http://www.cabforum.org for current version
[22] Lov 15.juni 2018 nr 38 om behandling av personopplysninger (personopplysningsloven)
[23] Forskrift 15.juni 2018 nr 876 om behandling av personopplysninger (personopplysningsforskriften)
[24] IETF RFC 4366: Transport Layer Security (TLS) Extensions, April 2006
[25] IETF RFC 6962: Certificate Transparency, June 2013
[26] IETF RFC 8555: Automatic Certificate Management Environment (ACME) March 2019

1.6.3 Conventions

Text that is outside text boxes is the Certificate Policy [18]. All Certificate Policy requirements contain either a SHALL, SHALL NOT, SHOULD, SHOULD NOT or MAY statement.

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

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

Hereinafter the term Certificate is used synonymously with Buypass ACME Certificates.

2 Publication and repository responsibilities

2.1 Publication of information

a) The Certificate Policy for Buypass ACME Certificates [18], the Certification Practice Statement for Buypass ACME Certificates [19] SHALL be publicly available on the Buypass Web 24x7.

The Certificate Policy for Buypass ACME Certificates [18] and the Certification Practice Statement for Buypass ACME Certificates [19] are available 24x7 and accessible on the Buypass Web.

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

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

2.2 Time or frequency of publication

The CA SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of Baseline Requirements [21].

The Certificate Policy for Buypass ACME SSL Certificates [18] and the Certification Practice Statement for Buypass ACME SSL Certificates [19] are updated regularly and when required due to changes in the Baseline Requirements [21].

2.3 Access controls on repositories

Refer to section 2.1.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

Refer to section 7.

3.1.2 Need for names to be meaningful

Refer to section 7.

3.1.3 Anonymity or pseudonymity of subscribers

Not used.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

Refer to section 7.

3.1.6 Recognition, authentication, and role of trademarks

Not used.

3.2 Initial identity validation

3.2.1 Method to Prove Possession of Private Key

a) 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. The Certificate Application including the CSR is also signed by the ACME Account Private Key.

b) 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 is rejected and the Certificate Applicant is notified without undue delay.

3.2.2 Authentication of Organization Identity

a) The following Subscriber information SHALL be obtained by the RA during initial registration
   - credentials for authenticating the Subscriber
   - contact information of Subscriber representatives acting as Subject Sponsor

Prior to, or at the time of submitting a Certificate Application, the Subscriber registers/confirms the following information using the ACME protocol:

- ACME Account Public Key according to ACME protocol specifications
- Contact information for the Subject Sponsor, i.e. phone number and/or e-mail address

b) All information provided SHALL be verified according to 4.1.1.

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

3.2.2.1 Identity
Not used.

3.2.2.2 DBA/Tradename
Not used.

3.2.2.3 Verification of Country
Not used

3.2.2.4 Validation of Domain Authorization or Control
The CA SHALL confirm that prior to issuance, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed in CA/Browser Forums Baseline Requirements [21].

The domain validation methods used for Buypass ACME Certificates are according to Baseline Requirements subsections:

- 3.2.2.4.7 DNS Change
- 3.2.2.4.19 Agreed-Upon Change to Website

3.2.2.4.1 Validating the Subscriber as Domain Name Registrant
Not used

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact
Not used.

3.2.2.4.3 Phone Contact with Domain Contact
Not used.

3.2.2.4.4 Constructed email to Domain Contact
Not used.

3.2.2.4.5 Domain Authorization Document
Not used.

3.2.2.4.6 Agreed-Upon Change to Website
Not used.

3.2.2.4.7 DNS Change
Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

This method is implemented according to DNS-01 in the ACME specification [26].

3.2.2.4.8 IP Address
Not used.

3.2.2.4.9 Test Certificate
Not used.

3.2.2.4.10 TLS Using a Random Number
Not used.

3.2.2.4.11 Any other method
Not used.

3.2.2.4.12 Validating Applicant as a Domain Contact
Not used.

3.2.2.4.13 Email to DNS CAA Contact
Not used.

3.2.2.4.14 Email to DNS TXT Contact
Not used.

3.2.2.4.15 Phone Contact with Domain Contact
Not used.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact
Not used.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact
Not used.

3.2.2.4.18 Agreed-Upon Change to Website v2
Not used.

3.2.2.4.19 Agreed-Upon Change to Website - ACME
Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555. The following are additive requirements to RFC 8555. The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received). The token (as defined in RFC 8555, section 8.3) MUST NOT be used for more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS. This method is NOT suitable for validating Wildcard Domain Names.

This method is implemented according to HTTP-01 in the ACME specification [26] and is not used for wildcard Domain Names.

3.2.2.4.20 TLS Using ALPN
Not used.

3.2.2.5 Authentication for an IP Address
Not used.

3.2.2.6 Wildcard Domain Validation.
Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the CA MUST establish and follow a documented procedure that determines if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix”.

Buypass ACME Certificates do not allow for wildcard character.

3.2.2.7 Data Source Accuracy

3.2.2.8 CAA Records
a) The CA MUST check for a CAA record for each domain in the certificate to be issued according to the procedure in RFC 8659 [14] and follow the processing instructions set down in RFC 8659 for any records found.

Buypass checks for CAA records for each domain registered by the Subscriber prior to issuance of a certificate. Buypass acts in accordance with the RFC 8659 [14] for any CAA records found.

b) The CA SHALL specify the set of issuer domain names that the CA recognizes in the CAA “issue” or “issuewild” records as permitting it to issue.

Buypass recognizes the issuer domain names ‘buypass.no’ and ‘buypass.com’ in the CAA records as authorization to issue certificates for the registered domain.

3.2.3 Authentication of Individual Identity
Not used.

3.2.4 Non-verified Subscriber Information
Not used.

3.2.5 Validation of Authority
The RA SHALL be able to identify the Subject Sponsor as an Authorized Subscriber Representative;

The ACME client and the registered ACME Account Key represent the Subscriber and the Subject Sponsor. All transactions in the ACME protocol are signed by the ACME Account Private Key and authenticate the Subject Sponsor and authorize the transaction appropriately.

3.2.6 Criteria for Interoperation or Certification
No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and Authentication for Routine Re-key
The requirements for identification and authentication of Subscriber and Authorized Subscriber Representatives are the same as for initial registration (refer to section 3.2).

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

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

3.3.2 Identification and Authentication for Re-key After Revocation
The requirements for identification and authentication of Subscriber and Authorized Subscriber Representatives are the same as for initial registration (refer to section 3.2).

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

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

3.4 Identification and authentication for revocation request
a) Only Authorized Subscriber Representatives MAY request Certificate revocation on behalf of the Subscriber.

A revocation request may be submitted from an ACME client to Buypass using the ACME protocol. To be authorized, the revocation request must be signed by the ACME Account Private Key.

Subscribers can also submit revocation requests to Buypass' revocation service by phone or by contacting the revocation service on Buypass Web. Once a revocation request is received, Buypass will attempt to obtain an authenticated confirmation from one of the Authorized Subscriber Representatives (Certificate Applicant, Certificate Manager, Certificate Approver or a Contract Signer) already registered with Buypass for that particular Subscriber and Certificate.

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

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

Refer to section 3.2.5

4 Certificate life-cycle operational requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The application procedure consists of the following main steps:

a) Subscriber Registration: The Subscriber must register Subscriber information with Buypass as defined in 3.1.1 using the ACME protocol.

b) Certificate Application including Certificate Signing Request Submission using the ACME protocol. The application request must be signed by the ACME Account Private Key.

4.1.2 Enrollment Process and Responsibilities

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

Terms and conditions regarding the use of the Certificates are made available to the Subscriber through a Subscriber Agreement. The Subscriber must accept the terms and conditions before it is possible to apply for a Certificate.

b) The Subscriber SHALL provide to the RA:
- all Subscriber information as defined in3.2
- the Subscriber's explicit consent to all terms and conditions regarding the use of the Certificate as defined in the Subscriber Agreement

All Subscriber information defined in 3.2 must be registered with Buypass using the ACME protocol and the Subscriber must explicitly give his/her consent to the Subscriber Agreement.

c) 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.

All data exchanged between the ACME Client and Buypass are protected by TLS.

4.2 Certificate application processing

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.

The Certificate Signing Request is an integral part of the Certificate Application that is submitted. All transactions are signed by the ACME Account Private Key.

b) The controls and procedures used to verify the Certificate Application SHALL conform to the information verification requirements defined by the CA/Browser Forum Baseline Requirements [21]

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

- all mandatory Subscriber information (refer to section 3.1.1) has been obtained from the Subscriber
- all transactions are signed by the ACME Account Private Key

Each of the above controls is performed according to verification methods that have been defined as acceptable by the CA/Browser Forum Baseline Requirements [21].

The domain validation methods used for Buypass ACME Certificates are described in 3.2.2.4.

If a domain is classified as a high risk domain, the certificate request will be rejected.

4.2.1 Performing Identification and Authentication Functions

For validation of Domain Names according to section 3.2.2.4, any reused data, document, or completed validation MUST be obtained no more than 398 days prior to issuing the Certificate

If the age of the domain validation exceed 180 days, the Domain Names will be revalidated before the certificate is issued.

4.2.2 Approval or Rejection of Certificate Applications

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

The verification controls have been implemented using automated system controls.

Automated verification controls performed in-line during a Subscriber's use of the ACME Protocol will result in immediate rejection of the Certificate Application.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA Actions during Certificate Issuance

a) 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.

b) The CA SHOULD NOT issue Certificates containing a new gTLD under consideration by ICANN.

Buypass only issue Certificates with gTLDs included in the IANA Root Zone Database.

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

All Buypass ACME Certificates that are issued follow the Buypass ACME Certificate profile referenced in section 7.

d) The validity period for a Buypass ACME Certificate SHALL NOT exceed 398 days. The age of validated data to support issuance of a Buypass ACME Certificate SHALL NOT exceeds 398 days, see [21].

Buypass ACME Certificates have a validity period of 180 days.

If the age of validated data supporting issuance of a new Buypass ACME Certificate exceeds 180 days, the data will be revalidated before the Certificate Application is processed and the certificate issued.

e) All SSL Certificates issued after 30 April 2018 MUST be compliant with Certificate Transparency requirements according to [25].

When a Certificate is to be issued, a precertificate is generated and registered in a number of CT-logs according to Chromium CT Policy. Each CT-log returns a signed certificate timestamp (SCT) as a proof of inclusion.

The precertificate is constructed from the certificate to be issued by adding a special poison extension (OID 1.3.6.1.4.1.11129.2.4.3). The precertificate is signed by the same CA issuing the final certificate.

The SCTs are embedded into the final certificate as a certificate extension (OID 1.3.6.1.4.1.11129.2.4.2).

4.3.2 Notification of Certificate Issuance
Not used.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance
The Subscriber SHALL review and verify the accuracy of the data in each SSL Certificate that it receives.

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.

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

4.4.2 Publication of the certificate by the CA
The CA SHALL ensure that the Certificates issued are made available as necessary to Subscribers and Relying parties.

Every Buypass ACME Certificate that is issued is distributed to the Subscriber through the ACME Protocol.

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

4.4.3 Notification of certificate issuance by the CA to other entities
Not used.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage
Refer to section 6.1.7 and 9.6.3.

4.5.2 Relying party public key and certificate usage
Refer to section 9.6.4.

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

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

The Subscriber handles renewal using the same procedure as for the initial application, refer to section 4.1.1.

4.6.1 Circumstance for certificate renewal
No stipulation.

4.6.2 Who may request renewal
No stipulation.

4.6.3 Processing certificate renewal requests
No stipulation.

4.6.4 Notification of new certificate issuance to subscriber
No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate
No stipulation.

4.6.6 Publication of the renewal certificate by the CA
No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities
Not used.

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

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

The Subscriber handles rekey using the same procedure as for the initial application, refer to section 4.1.1.

4.7.1 Circumstance for certificate re-key
No stipulation.

4.7.2 Who may request certification of a new public key
No stipulation.

4.7.3 Processing certificate re-keying requests
No stipulation.

4.7.4 Notification of new certificate issuance to subscriber
No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate
No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA
No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities
Not used.

4.8 Certificate modification
4.8.1 Circumstance for certificate modification
Not used.

4.8.2 Who may request certificate modification
Not used.

4.8.3 Processing certificate modification requests
Not used.

4.8.4 Notification of new certificate issuance to subscriber
Not used.

4.8.5 Conduct constituting acceptance of modified certificate
Not used.

4.8.6 Publication of the modified certificate by the CA
Not used.

4.8.7 Notification of certificate issuance by the CA to other entities

Not used.

4.9 Certificate revocation and suspension

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

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

Buypass offers a service that accepts revocation requests through the ACME Protocol and this service is available 24x7

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

Buypass also offers a 24x7 problem reporting service where Subscribers, Relying Parties and other third parties can report complaints or suspected Private Key compromise, SSL Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to SSL Certificates. The problem reporting service is also available by phone or on the Buypass Web. 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 Baseline Requirements [21]. Also refer to section 1.5.2.

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 if the reason for revocation is critical and at most 5 days otherwise (refer to section 4.9.1).

Revocation requests through the ACME Protocol are verified and processed immediately.

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

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

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

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

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

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

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

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

d) The CA SHALL operate and maintain its revocation status services with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

Buypass offers a CRL service and an OCSP service where the response time is less than ten seconds.

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

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

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

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

g) A revoked Certificate SHALL NOT be reinstated.

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

a) The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:
- the Subscriber requests revocation of its Certificate
- the Subscriber notifies the CA that the original Certificate Application was not authorized and does not retroactively grant authorization
- the CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate has been compromised
- The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

b) The CA SHOULD revoke a Certificate within 24 hours and MUST revoke a Certificate within 5 days if one or more of the following occurs:
- The Certificate no longer complies with the requirements of 6.1.5 and 6.1.6
- The CA obtains evidence that the Certificate was misused
- the CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement
- the CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name)
- the CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name
- the CA is made aware of a material change in the information contained in the Certificate
- the CA is made aware that the Certificate was not issued in accordance with the applicable Certificate Policy [18] or the Certification Practice Statement [19]
- the CA determines that any of the information appearing in the Certificate is inaccurate
- the CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate
- the CA's right to issue Certificates under CA/Browser Forum Baseline Requirements (see [21] expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository

- Revocation is required by the Issuing CA's Certificate Policy [19] and/or Certification Practice Statement [20]
- The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, or if there is clear evidence that the specific method used to generate the Private Key was flawed
- the Subscriber does not pay the service fees to Buypass (refer to section 9.1.1)

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

- the Subordinate CA requests revocation in writing
- the Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization
- the Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Subordinate CA Certificate has been compromised or no longer complies with the requirements of 6.1.5 and 6.1.6
- the Issuing CA obtains evidence that the Subordinate CA Certificate was misused
- the Issuing CA is made aware that the Subordinate CA Certificate was not issued in accordance with or that Subordinate CA has not complied with the Certificate Policy [18] or Certification Practice Statement [19]
- the Issuing CA determines that any of the information appearing in the Subordinate CA Certificate is inaccurate
- the Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Subordinate CA Certificate
- the Issuing CA's or Subordinate CA's right to issue Certificates under CA/Browser Forum Baseline Requirements (see [21]) expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository
- Revocation is required by the Issuing CA's Certificate Policy [18] and/or Certification Practice Statement [19]

4.9.2 Who Can Request Revocation

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

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

Buypass accepts revocation requests from previously unregistered Subscriber Representatives only if

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

b) Buypass, through further investigation, has reason to believe that a valid revocation reason exists (refer to section 4.9.1).

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

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

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

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

4.9.3 Procedure for Revocation Request

The CA SHALL provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in the CA's Certificate Policy or Certification Practice Statement. The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

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

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

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

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

c) All previously revoked Buypass SSL Evident Certificates and previously rejected Buypass SSL Evident 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 Buypass SSL Evident Certificates and previously rejected Buypass SSL Evident 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.

d) The CA SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA SHALL publicly disclose the instructions through a readily accessible online means and in section 1.5.2 of their CPS.

Refer to section 1.5.2 and 4.9 a).

4.9.4 Revocation Request Grace Period

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

b) For revocation reason key compromise, refer to section 4.9.12.

4.9.5 Time within which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the CA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1. The date selected by the CA SHOULD consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
5. Relevant legislation.

Buypass will start investigate a Certificate Problem Report as soon as possible and within 24 hours after receiving a Problem Report provide a preliminary report to the entity who filed the Problem Report and the Subscriber if this is considered necessary.

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 CRL Issuance Frequency

a) The CA SHALL provide a CRL service.

Buypass provides a CRL service where CRLs may be accessed using the HTTP protocol. The HTTP URL is included in the CRL Distribution Point extension of all Certificates that are issued and the URL is also available on Buypass Web.

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

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

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

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

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

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-line Revocation/Status Checking Availability

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

Buypass provides an online OCSP service. The service URL is included in the AIA extension of all Certificates and the URL is also available on Buypass Web.

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

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

c) The CA SHALL update information provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.

The revocation status information from the OCSP service is updated at least every 24 hours for both Subscriber Certificates and Subordinate CA Certificates.

d) The CA SHALL support an OCSP capability using the GET method for Certificates issued.

The OCSP service supports the GET method.

e) If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder SHOULD NOT respond with a "good" status. The CA SHOULD monitor the responder for such requests as part of its security response procedures.

The OCSP service responds with an “unknown” status if the requested certificate has not been issued. Such requests are being monitored 24x7.

f) If the Subscriber Certificate is for a high-traffic FQDN, the CA MAY rely on stapling, in accordance with RFC4366 [22], to distribute its OCSP responses.

We do not rely on stapling or require this to be performed by Subscribers.

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

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

4.9.10 On-line Revocation Checking Requirements

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

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

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

Subscribers may report private key compromise to Buypass as a revocation request, see 4.9.1 and 4.9.2.

b) A CA MUST clearly specify the methods that parties may use to demonstrate private key compromise.

Other parties may report private key compromise using one of the following methods:

a) By returning a CSR signed by the compromised private key using a challenge provided by Buypass as Common Name; or

b) By providing the private key itself

Private key compromise should be reported by using SSL Problem reporting mechanism as specified in 1.5.2.

4.9.13 Circumstances for Suspension
Not used.

4.9.14 Who Can Request Suspension
Not used.

4.9.15 Procedure for Suspension Request
Not used.

4.9.16 Limits on Suspension Period
Not used.

4.10 Certificate status services

4.10.1 Operational Characteristics
Refer to section 4.9.7 and 4.9.9.

4.10.2 Service Availability
Refer to section 4.9.7 and 4.9.9.

4.10.3 Optional Features
No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices
Not used.

4.12.2 Session key encapsulation and recovery policy and practices
Not used.

5 Management, operational, and physical controls

a) The CA SHALL implement Computer Security Controls according to best practice according to ISO/IEC 27002:2013[8] and in compliance with Buypass Information Security Policy [20].

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

Buypass' ISMS is reasonably designed to:

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

d) Comply with the security requirements defined by ETSI EN 319 401 [15], ETSI EN 319 411-1 [16] and ETSI EN 319 411-2 [17];

e) 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 Data, issues SSL Certificates, maintains a Repository, and revokes SSL Certificates;

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

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

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

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

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

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

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

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

5.1 Physical security Controls

5.1.1 Site location and construction

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

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

5.1.2 Physical access

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

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

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

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

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

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

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

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

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

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

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

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

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

5.1.3 Power and air conditioning
No stipulation.

5.1.4 Water exposures
No stipulation.

5.1.5 Fire prevention and protection
No stipulation.

5.1.6 Media storage
No stipulation.

5.1.7 Waste disposal
No stipulation.

5.1.8 Off-site backup
No stipulation.

5.2 Procedural controls

5.2.1 Trusted Roles

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

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

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

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

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

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

5.2.2 Number of Individuals Required per Task

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

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

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

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

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

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

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

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

5.2.3 Identification and Authentication for Trusted Roles

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

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

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

5.2.4 Roles Requiring Separation of Duties

Refer to section 5.2.1.

5.3 Personnel controls

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

5.3.1 Qualifications, Experience, and Clearance Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

5.3.2 Background Check Procedures

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

Refer to section 5.3.1 a)

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

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

5.3.3 Training Requirements and Procedures

No stipulation.

5.3.4 Retraining Frequency and Requirements

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

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

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

a) Appropriate disciplinary sanctions SHALL be applied to personnel violating the Certificate Policy [18] or underlying operative procedures.

Buypass' Chief Security Officer is responsible for making trusted personnel aware of consequences and disciplinary actions as a result of security violations as seen in the context of the Certification Practice Statement [19] and supporting operational routines.

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

Routines are in place that promptly enables Buypass to revoke a person's access to Buypass facilities and systems if it is revealed that a trusted person has acted in an unauthorized manner and/or in a way that that

Buypass no longer has necessary trust in this person. A decision to revoke a person's access is taken by the Buypass' Operations Manager together with Buypass' Chief Security Officer.

5.3.7 Independent Contractor Controls

Independent contractors or consultants MAY possess trusted positions subject to the contractors or consultants being trusted by the CA to the same extent as if they were employees. Otherwise, independent

contractors and consultants shall have access to secure facilities only to the extent they are escorted and directly supervised by Trusted Personnel.

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

5.3.8 Documentation Supplied to Personnel

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

Buypass ensures that all employees are familiar with the Buypass' information security policy and that employees involved in the provisioning of CA/RA services as specified in 9.6 are familiar with the Certificate Policy [18] and the Certification Practice Statement [19]. Both documents are available electronically.

5.4 Audit logging procedures

5.4.1 Types of Events Recorded

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

a) The CA SHALL record in details of the actions taken to process an Certificate Application and to issue an SSL Certificate, including all information generated and documentation ~~or~~ received in connection with an SSL Certificate Application, including time and date, and personnel involved. The CA SHALL make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

Refer to section 5.4.1 g)

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

c) All registration information including the following shall be recorded:
   1. type of document(s) presented by the applicant to support registration;
   2. record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;
   3. storage location of copies of applications and identification documents, including the signed Subscriber Agreement
   4. identity of entity accepting the application;
   5. method used to validate identification documents, if any; and
   6. name of receiving CA and/or submitting Registration Authority, if applicable.

Refer to section 5.4.1 g)

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

Refer to section 5.4.1 g)

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

Buypass records the Subscriber Agreement signed by the authorized Contract Signer – refer to section 4.1.2

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

Refer to section 9.4

g) The record requirements in a) include, but are not limited to, an obligation to record the following events:
   1. CA certificate and key lifecycle events, including:
      - Key generation, backup, storage, recovery, archival, and destruction;
      - Certificate requests, renewal, and re-key requests, and revocation;
      - Approval and rejection of certificate requests;
      - Cryptographic device lifecycle management events;
      - Generation of Certificate Revocation Lists and OCSP entries;
      - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
   2. Subscriber Certificate lifecycle management events, including:
      - Certificate requests, renewal, and re-key requests, and revocation;
      - All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
      - Approval and rejection of certificate requests;
      - Issuance of Certificates; and
      - Generation of Certificate Revocation Lists and OCSP entries.
   3. Security events, including:
      - Successful and unsuccessful PKI system access attempts;
      - PKI and security system actions performed;
      - Security profile changes;
      - Installation, update and removal of software on a Certificate System;
      - System crashes, hardware failures, and other anomalies;
      - Firewall and router activities; and
      - Entries to and exits from the CA facility.

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

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

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

Refer to section 4.5.1 b)

5.4.2 Frequency for Processing and Archiving Audit Logs

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

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

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

b) Other audit logs SHALL be processed as needed.

Refer to section 5.4.2 a)

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

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

5.4.3 Retention Period for Audit Logs

Refer to section 5.5.2.

The CA SHALL retain, for at least two years:

- CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of:
    a. the destruction of the CA Private Key; or
    b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
- Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 (2)) after the revocation or expiration of the Subscriber Certificate.
- Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

Refer to section 5.5.2

5.4.4 Protection of Audit Log

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

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

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

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

5.4.5 Audit Log Backup Procedures

There SHALL be offsite backup of all audit logs.

Buypass performs regular off-site backup of all security relevant audit logs. Also refer to section 5.4.4 a)

5.4.6 Audit Log Accumulation System (internal vs. external)

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

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

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

5.5 Records archival

5.5.1 Types of Records Archived

No stipulation.

5.5.2 Retention Period for Archive

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

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

5.5.3 Protection of Archive

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

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

5.5.4 Archive Backup Procedures

Refer to 5.4.5.

5.5.5 Requirements for Time-stamping of Records

No stipulation.

5.5.6 Archive Collection System (internal or external)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

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

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

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

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

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

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

5.6 Key changeover

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

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

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

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

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

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

Refer to section 6.1.4

5.7 Compromise and disaster recovery

5.7.1 Incident and Compromise Handling Procedures

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

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

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

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

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

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

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

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

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

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

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

5.7.3 Recovery Procedures After Key Compromise

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

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

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

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

5.7.4 Business Continuity Capabilities after a Disaster

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

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

5.8 CA or RA termination

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

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

Buypass has a Buypass CA termination plan.

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

The Buypass CA termination plan includes all requirements above.

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

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

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

The provisions are stated in the Buypass CA termination plan.

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

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

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Root CA key generation

a) For Root CA Key Pairs the CA SHALL:
1. prepare and follow a Key Generation Script,
2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process, and
3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

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

Ceremonies involving generation of Root CA Private Keys are under supervision of a Qualified Auditor.

CA key generation

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

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

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

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

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

Buypass produces a ceremony report signed by all participants of the ceremony

e) The CA private signing key SHALL be generated within a cryptographic device which either:
- meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3] level 3 or higher; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [10], or equivalent security criteria.

The Buypass Class 2 CA Private Keys are generated in a HSM compliant to FIPS 140-2 level 3.

f) 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 [18].

Refer to section 5.6.

6.1.1.2 RA Key Pair Generation

Not used.

6.1.1.3 Subscriber Key Pair Generation

a) The CA SHALL reject a certificate request if one or more of the following conditions are met:
   1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
   2. There is clear evidence that the specific method used to generate the Private Key was flawed;
   3. The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
   4. The CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;
   5. The CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

Buypass rejects certificate requests if the requirements in section 6.1.5 or 6.1.6 are not met.

Buypass rejects a certificate request if the corresponding private key previously have been reported as compromised, i.e. as described in 4.9.12.

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

b) If the Subscriber Certificate will contain an extKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280], the CA SHALL NOT generate a Key Pair on behalf of a Subscriber, and SHALL NOT accept a certificate request using a Key Pair previously generated by the CA.

Buypass does not generate a Key Pair on behalf of the Subscriber.

6.1.2 Private Key Delivery to Subscriber

Not used.

6.1.3 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:

- authenticate the Subscriber as the originator of the request
- 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. Otherwise, the Public Key is included in the Certificate Application as described in 4.1 and its origin will be verified as a part of this.

6.1.4 CA Public Key Delivery to Relying Parties

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

The Root Certificate is pre-installed in common OS, browsers and web server software by the applicable software vendors.

Both the issuing CA and Root CA Certificates may also be downloaded from Buypass Web. Both certificates' fingerprints are included on the website.

b) If a self-signed certificate is issued by the CA, the attributes of the certificate shall be compliant with the defined key usage as defined in Recommendation ITU-T X.509 [6]

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

6.1.5 Key Sizes

a) For RSA key pairs the CA SHALL:
   - Ensure that the modulus size, when encoded, is at least 2048 bits, and;
   - Ensure that the modulus size, in bits, is evenly divisible by 8.

b) For ECDSA key pairs, the CA SHALL:
   - Ensure that the key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve.

No other algorithms or key sizes are permitted

Root CA and CA keys

c) CA key pair generation SHOULD be performed using an algorithm as specified in ETSI TS 119 312 [9] for the CA's signing purposes.

d) The selected key length and algorithm for CA signing key SHOULD be one which is specified in ETSI TS 119 312 [9] for the CA's signing purposes.

CA signature keys for are RSA 4096 bits.

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

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

Subject keys

e) Subject keys shall be generated using an algorithm recognized as being fit for the uses identified in this Certificate Policy during the validity time of the Certificate, see [9].

f) Subject keys SHOULD be of a key length and for use with a public key algorithm as specified in ETSI TS 119 312 [9] for the purposes stated in this Certificate Policy during the validity time of the certificate.

Buypass supports only RSA and ECC Subject keys.

Upon reception of a Certificate Signing Request, Buypass verifies that the key is either NIST P-256 (ECC) or minimum RSA 2048 bits. In addition, the RSA modulus size must be divisible by 8.

6.1.6 Public Key Parameters Generation and Quality Checking

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

Additionally, the public exponent SHOULD be in the range between 2^16 + 1 and 2^256 - 1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

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

6.1.7 Key Usage Purposes

Root CA keys

a) Private Keys corresponding to Root Certificates MUST NOT be used to sign Certificates except for Subordinate CA Certificates and delegated OCSP Responder certificates.

The Buypass Class 2 Root CA Private Key is used to sign Intermediate CA Certificates, OCSP Responder certificates and CRLs.

CA keys

b) 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 and CRLs.

The Buypass Class 2 CA 5 Private Key is used to sign precertificates according to Certificate Transparency (see [25]).

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

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

Subject keys

d) Key usage combinations SHALL be set according to[5] and compliant with [4].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

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

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

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

Refer to section 6.2.1 a) and c)

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

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

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

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

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

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

f) The secure cryptographic module shall be functioning correctly.

All HSMs are verified for correctness at startup.

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

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

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

Refer to section 6.1.1, 6.2.4 and 6.2.7

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

6.2.3 Private Key Escrow

Not used.

6.2.4 Private Key Backup

CA key backup

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

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

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

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

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

Se 6.2.4 b).

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

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

6.2.5 Private Key Archival

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

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

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

Refer to section 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.

Refer to section 6.2.4 d).

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

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

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

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

Refer to section 6.1.1.1 and 6.2.4

The CA Private Key is generated within a cryptographic module.

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

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Activating Private Keys

CA Private Key

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

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

Subject Private Key

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

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

6.2.9 Deactivating Private Keys

No stipulation.

6.2.10 Destroying Private Keys

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

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

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

6.2.11 Cryptographic Module Capabilities
No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public Key Archival
No stipulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods
The Certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the Certificate. The validity period is stated in the Validity field of the Certificate.

CA keys

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

The signing key for Buypass Class 2 CA 5 has a lifetime of 10 years. The signing key for Buypass Class 2 Root CA has a lifetime of 30 years.

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

The CA Public Keys may be used for verification purposes beyond the CA certificate validity period.

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

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

b) Activation Data protecting access to Subject Private Keys SHOULD be a strong password/PIN that cannot be easily guessed. 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.

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

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

6.4.3 Other aspects of activation data
No stipulation.

6.5 Computer security controls

6.5.1 Specific Computer Security Technical Requirements
a) The Computer Security Controls SHALL conform to the Normalized Certificate Policy (NCP) requirements of ETSI EN 319 411-1 [16].

Refer to section 5 a).

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

Refer to section 5 a).

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

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

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

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

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

Revocation status information is protected from being modified.

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

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

6.5.2 Computer Security Rating
No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls
The CA SHALL implement Life Cycle Security Controls according to best practice according to ISO/IEC 27002:2013 [6] and in compliance with Buypass Information Security Policy [20].

Systems development and maintenance activities are designed to maintain CA system integrity. Strict control is maintained over access to program source libraries. Formal change control procedures exist and are followed for the implementation of software, scheduled software releases and emergency software fixes. Also refer to section 5 a).

6.6.2 Security management controls
No stipulation.

6.6.3 Life cycle security controls

a) The Computer Security Controls SHALL conform to the Normalized Certificate Policy (NCP) requirements of ETSI EN 319 411-1 [16].

Refer to section 5 a).

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

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

6.7 Network security controls

a) The CA SHALL implement Network Security Controls according to best practice according to ISO/IEC 27002:2013 [8] and in compliance with Buypass Information Security Policy [20].

Refer to section 5 a).

b) The Network Security Controls SHALL conform to the requirements defined by the policy for EU qualified website certificates (QCP-w) [17].

Refer to section 5 a).

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

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

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

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

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

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

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

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

6.8 Time-stamping

No stipulation.

7 Certificate, CRL, and OCSP profiles

The Certificate, CRL and OCSP profiles SHALL be described in the Buypass Class 2 Certificate and CRL profiles [5] and the document SHALL be made publicly available at Buypass Web.

7.1 Certificate profile

The certificates shall meet the requirements, specified in Recommendation ITU-T X.509 [6] or IETF RFC 5280 [12].

The Certificate profile for Buypass Class 2 SSL Certificates SHALL conform to the current version of the CA/Browser Forum Baseline Requirements [21].

7.1.1 Version Number(s)

Refer to Buypass Class 2 Certificate and CRL profiles [5].

7.1.2 Certificate Extensions

Refer to Buypass Class 2 Certificate and CRL profiles [5].

7.1.3 Algorithm Object Identifiers

Refer to Buypass Class 2 Certificate and CRL profiles [5].

7.1.4 Name Forms

Refer to Buypass Class 2 Certificate and CRL profiles [5].

7.1.5 Name Constraints

Refer to Buypass Class 2 Certificate and CRL profiles [5].

7.1.6 Certificate Policy Object Identifier

Refer to Buypass Class 2 Certificate and CRL profiles [5].

7.1.7 Usage of Policy Constraints Extension

Not used.

7.1.8 Policy Qualifiers Syntax and Semantics

Refer to Buypass Class 2 Certificate and CRL profiles [5].

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL profile

The CRL shall be as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 [6] or IETF 5280 [12].

7.2.1 Version number(s)

Refer to Buypass Class 2 Certificate and CRL profiles [5].

7.2.2 CRL and CRL entry extensions

Refer to Buypass Class 2 Certificate and CRL profiles [5].

7.3 OCSP profile

The OCSP profile SHALL conform to the specifications contained in RFC 6960 [11].

7.3.1 Version number(s)

Refer to Buypass Class 2 Certificate and CRL profiles [5].

7.3.2 OCSP extensions

Refer to Buypass Class 2 Certificate and CRL profiles [5].

8 Compliance audit and other assessments

The CA SHALL at all times comply with audit requirements set forth in CA/Browser Forums Baseline Requirements [21].

The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.

8.1 Frequency or circumstances of assessment

The CA SHALL be audited once per calendar year for compliance with the practices and procedures set forth in the Certification Practice Statement for Buypass Class 2 SSL Certificates [19].

Buypass is audited annually for conformance to ETSI EN 319 401 [15], ETSI TS 319 411-1 [16] and ETSI EN 319 411-2 [17].

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

Go SSL Certificates are covered by the compliance certificate identified as ETS 018.

8.2 Identity/qualifications of assessor

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

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

8.3 Topics covered by assessment

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

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

The compliance certificates are compliant with the Mozilla Root Store Policy.

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

8.4 Actions taken as a result of deficiency

No stipulation.

8.5 Communication of results

No stipulation.

8.6 Self-Audits

During the period in which the CA issues Certificates, the CA SHALL monitor adherence to its Certificate Policy,Certification Practice Statement and CA/Browser Forums Baseline Requirements [21]. The CA SHALL strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Buypass performs self audits on a quarterly basis of three percent of the SSL Business and three percent of SSL Domain certificates. Samples are selected randomly.

The self audits are performed according to a defined procedure.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

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

The service fees charged by Buypass for Buypass ACME Certificates are published on the Buypass Web.

9.1.2 Certificate access fees

Not used.

9.1.3 Revocation or status information access fees

Not used.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

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

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

The following information is not considered confidential/private;

- Certificates
- Certificate revocation status information

All other information about Subscribers, Subscriber Representatives and their use of Buypass services will be treated as confidential/private by Buypass. Buypass handles private information according to [22] and [23].

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information
No stipulation.

9.4 Privacy of personal information

Buypass complies with the Norwegian law related to general data protection regulation, see [22] and [23].

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

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

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

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

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

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

9.4.2 Information treated as private
No stipulation.

9.4.3 Information not deemed private
No stipulation.

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

Refer to section 9.3.1.

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

Refer to section 9.4.6.

9.4.5 Notice and consent to use private information
No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process
Buypass SHALL have the right to release information that is considered confidential to law enforcement officials in compliance with Norwegian law.

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

9.4.7 Other information disclosure circumstances

9.5 Intellectual property rights

a) Key pairs corresponding to Buypass CA Certificates SHALL be the property of Buypass. Key pairs corresponding to Buypass 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 [18] and the Certification Practice Statement [19].

9.6 Representations and warranties

Buypass operates as both the CA and RA for all Certificates issued under the Certificate Policy [18] and thereby fulfills all CA and RA obligations in this section.

9.6.1 CA Representations and Warranties

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

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

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate.

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with the Certificate Policy for Buypass Class 2 SSL Certificates [18] and consistent with the Certification Practice Statement for Buypass Class 2 SSL Certificates [19] in issuing and managing the Certificate.

The CA SHALL warrant that the identity of the Subscriber that appears in an issued Buypass SSL Business Certificate is accurate and correct at the time of issuance. The CA SHALL warrant that any other information contained in the certificate is accurate and not misleading.

The CA SHALL warrant that at the time of issuance the Subscriber authorized the issuance of the Certificate and that the applicant representative is authorized to request the Certificate on behalf of the Subscriber.

The CA SHALL warrant that the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement.

The CA SHALL warrant that the Subscriber, at the time of issuance, either had the right to use, or had control of, the Domain Name(s) listed in the Certificate - or was delegated such right or control by someone who had such right to use or control.

The CA will revoke the Certificate for any of the reasons specified in this document.

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 Baseline Requirements [21].

The CA SHALL provide the capability to allow third parties to check and test all the Certificate types that the CA issues. Any test certificates should clearly indicate that they are for testing purposes (e.g. by the subject name).

9.6.2 RA Representations and Warranties

An RA operating under the Certificate Policy for Buypass ACME Certificates [18] SHALL:

- receive Certificate Applications from Subscribers, both initial applications (refer to section 4.1.1) and rekey applications (refer to section 4.7)
- verify all information submitted by Subscribers, both for initial applications and for rekey applications and if such verification is successful, submit a request to the CA for the issuance of a Buypass ACME Certificate
- receive and verify requests from Subscribers for the revocation of Buypass ACME Certificates, and if the verification of a revocation request is successful, submit a request to the CA for the revocation of that Certificate

9.6.3 Subscriber Representations and Warranties

The CA SHALL require, as part of the Subscriber Agreement that the Subscriber make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, the Subscriber's agreement to the Subscriber Agreement with the CA.

The CA SHALL implement a process to ensure that each Subscriber Agreement is legally enforceable against the Subscriber. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request.

The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Subscriber is clearly covered by that Subscriber Agreement.

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

- submit accurate and complete information to the CA in accordance with the requirements in the Certification Practice Statement for Buypass ACME Certificates [19]
- maintain correct Subscriber information, and notify the RA or CA of any changes to this information
- notify the CA if any information in the Certificate is incorrect
- acknowledge and accept that the CA is entitled to revoke the certificate immediately if the Subscriber were to violate the terms of the Subscriber Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware

- request the Certificate to be revoked when a valid revocation reason exists (refer to section 4.9.1.1)
- inform the CA whenever an Authorized Subscriber Representative no longer is authorized to represent the Subscriber
- ensure that the Private Keys and Certificates are only used in accordance with any limitations notified to the Subscriber
- install the SSL Certificate only on the server accessible at the domain name listed in the SSL Certificate
- take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token)
- ensure that the key generation and the Private Key satisfies the requirements in 6.1.1.3 and 6.1.5
- the use of the Private Key is immediately and permanently discontinued if the Private Key is compromised or the Certificate is revoked
- not install or use the SSL Certificate until it has been reviewed and the accuracy of the data in the SSL Certificate has been verified
- respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period
- in the case of being informed that the CA has been compromised, ensure that the Private Key is no longer used
- inform the Subject Sponsor(s) of all obligations applicable to the Subject

9.6.4 Relying Party Representations and Warranties

A Relying Party is solely responsible for deciding whether or not to rely on Certificates issued under the Certificate Policy for Buypass ACME Certificates [18].

The Relying Party SHALL:

- restrict reliance on Buypass ACME Certificates to the purposes for those Certificates as defined by the Certificate Policy for Buypass ACME Certificates [18]
- acknowledge applicable liability caps and warranties as defined by the Certificate Policy for Buypass ACME Certificates [18]
- read and agree to all terms and conditions of the Buypass ACME Certificate Policy
- rely on a Buypass ACME 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 ACME Certificate and the value of any transaction that may involve the use of a Buypass ACME 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 ACME Certificates, including use of revocation services, in accordance with best practice certification path validation as defined by RFC 5280 [12]
- when verifying a digital signature, take into consideration all information in the Certificate, in this Policy and obey best practices for validating signatures

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

9.6.5 Representations and Warranties of Other Participants

The CA SHALL have a properly documented agreement and contractual relationship in place where the provisioning of CA/RA services (refer to section 9.6.1) involves subcontracting, outsourcing or other third party arrangements. The agreement SHALL include (directly or by reference) the applicable requirements of the CA/Browser Forums Baseline Requirement [21].

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 ACME Certificates.

9.7 Disclaimers of warranties

Issuance of Certificates in accordance with the Certificate Policy [18] SHALL NOT make the CA an agent, fiduciary, trustee, or other representative of Subscribers or Relying Parties

9.8 Limitations of liability

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

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

9.9 Indemnities

9.9.1 Indemnification by CAs

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, Buypass understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Buypass Root CA do not assume any obligation or potential liability of the CA under CA/Browser Forum Baseline Requirements [21] or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others.

Buypass defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by Buypass, regardless of the cause of action or legal theory involved.

This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by Buypass where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

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

- the Subscriber's failure to perform the obligations of a Subscriber as defined in 9.6.3
- falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application
- failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party
- the Subscriber's failure to protect the Subscriber's Private Key, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's Private Key
- 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

9.9.3 Indemnification by Relying Parties

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

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

The applicable Subscriber Agreement and/or Relying Party Agreement MAY include additional indemnity obligations

9.10 Term and termination

9.10.1 Term
No stipulation.

9.10.2 Termination
Refer to section 5.8.

9.10.3 Effect of termination and survival
Refer to section 5.8.

9.11 Individual notices and communications with participants

9.12 Amendments

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

Buypass Policy Board MAY amend the Certificate Policy [18] or the Certification Practice Statement [19] at its own discretion.

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

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

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

The CP and CPS are modified and approved by Buypass Policy Board in accordance with a defined review process. Also refer to section 1.5.4.

9.12.2 Notification mechanism and period
Minor changes to layout and text MAY be amended without further notice.

Buypass MAY change any part of the Certificate Policy [18] or the Certification Practice Statement [19] with 15 days advance notice.

Any change that may materially influence users of the Certificate Policy[18] or the Certification Practice Statement [19] SHALL be published on Buypass Web.

Users that are influenced by a change MAY comment upon it. Whether or not comments are honoured, SHALL solely be for Buypass Policy Board to decide. A change in the Certificate Policy [18] or the Certification Practice Statement [19] that is amended SHALL be subject to a new advance notice.

Modifications to either the Certificate Policy [18] or the Certification Practice Statement [19] that in the judgment of Buypass will have little or no impact on Subscribers and Relying Parties, may be made with no change in version number and no prior notification to Subscribers and Relying Parties. Such changes shall become effective immediately upon publication on the Buypass Web.

In the event that Buypass makes a significant modification to either the Certificate Policy [18] or the Certification Practice Statement [19] the respective document version number will be updated accordingly.

In this case a change notification will be published on the Buypass Web no later than 15 days before the new document version becomes effective.

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

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

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

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

In case of a dispute arising out of or in respect to any Buypass SSL Certificate or any services provided in respect to any Buypass SSL Certificate the parties SHALL try to settle the dispute through negotiations and conciliation. If the dispute is not resolved within 3 months from the commencement of the conciliatory process, each party has the right to bring the dispute to a Norwegian court for settlement. Oslo District Court shall be the exclusive first instance venue for all such disputes.

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

9.14 Governing law

The laws of the country of Norway SHALL govern the construction, validity, interpretation, enforceability and performance of the Certificate Policy [18], the Certification Practice Statement [19], all related Subscriber Agreements and all related Relying Party Agreements

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

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

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Severability
In the event that a clause or provision of the Certificate Policy [18] or the Certification Practice Statement [19] is held to be unenforceable by a court of law, the remainder of the respective Certificate Policy or Certification Practice Statement SHALL remain valid.

Survival
Subscribers and Relying Parties SHALL be bound by its terms for all SSL Certificates issued for the remainder of the validity periods of such Certificates, also upon termination or expiration of the Certificate Policy [18], the Certification Practice Statement [19] any Subscriber Agreements and any Relying Party Agreements.

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

Notice
Any notice to be given by a Subscriber, Applicant, or Relying Party to Buypass under the Certificate Policy [18], the Certification Practice Statement [19], a Subscriber Agreement, or a Relying Party Agreement SHALL be given in writing (e-mail, post, courier) to the contact point specified in 1.5.2.

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.