CERTIFICATE POLICY

BUYPASS CLASS 2 MERCHANT CERTIFICATES

Effective date: 28.04.2014

PUBLIC

Version: 2.0
Document date: 15.03.2014

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

Table of content

DEFINITIONS

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

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

REFERENCES

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

1 Introduction

1.1 Overview

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

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

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

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

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

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

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

1.1.1 How to read this document

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

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

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

Hereinafter the term Certificate is used synonymously with Buypass Class 2 Merchant Certificates.

1.2 Identification

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

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

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

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

1.3 Community and applicability

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

1.3.1 Applicability

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

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

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

1.4 Contact details

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

Contact point for questions regarding these documents is:

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

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

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

Buypass Kundeservice
Postboks 639
N-2810 Gjøvik

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

2 General provisions

2.1 Obligations

2.1.1 CA obligations

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

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

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

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

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

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

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

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

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

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

2.1.2 RA obligations

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

The RA SHALL:

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

2.1.3 Subscriber obligations

The Subscriber SHALL fulfill all obligations of the Subscriber Agreement.

The Subscriber SHALL:

- submit accurate and complete information to the CA in accordance with the requirements in the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19]
- maintain correct information about the Subscriber and Subject, and notify the RA or CA of any changes to this information
- request the Certificate to be revoked when a valid revocation reason exists (see 4.4.1)
- be responsible for ensuring that restrictions on Private Keys and Certificates use are maintained
- exercise reasonable care to avoid unauthorized use of the Subjects Private Keys
- inform the RA whenever an Authorized Subscriber Representative no longer is authorized to represent the Subscriber
- in the case of being informed that the CA has been compromised, ensure that the Private Key is no longer used by the Subject
- inform Certificate Applicant and Subject Sponsors of all obligations applicable to the Subject

2.1.4 Subcontractor obligations

The CA SHALL have a properly documented agreement and contractual relationship in place where the provision of services (see 2.1.1) involves subcontracting, outsourcing or other third party arrangements.

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

2.1.5 Relying Party obligations

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

The Relying Party SHALL:

- restrict reliance on Buypass Class 2 Merchant Certificates to the purposes for those Certificates as defined by section 1.3
- acknowledge applicable terms, conditions, warranties and liability caps as defined in section 2
- rely on a Buypass Class 2 Merchant Certificate only if such reliance is reasonable in the circumstances, including determining whether such reliance is reasonable given the nature of the security and trust provided by a Buypass Class 2 Merchant Certificate and the value of any transaction that may involve the use of a Buypass Class 2 Merchant Certificate
- consult the most recent revocation status information in order to establish whether any of the Certificates in the certification path have been revoked or suspended
- verify Buypass Class 2 Merchant Certificates, including use of revocation services, in accordance with best practice certification path validation as defined by RFC 5280 [20]

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

2.2 Liability

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

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

The CA has defined the following yearly liability caps:

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

- **for Relying Parties:** NOK 50.000,- for all digital signatures and transactions related to all Certificates for a given Relying Party per year

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

2.3 Financial responsibility

2.3.1 Indemnification of CA and RA by Relying Parties

Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers SHALL indemnify and hold Buypass harmless from and against any and all liabilities, losses, costs, expenses, damages, claims and settlement amounts arising out of or relating to any reliance by a Relying Party on any Buypass Class 2 Merchant Certificate or any service provided in respect to Buypass Class 2 Merchant Certificates for:

- the Subscriber's failure to perform the obligations of a Subscriber as defined in section 2.1.3

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

Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Parties SHALL indemnify and hold Buypass harmless from and against any and all liabilities, losses, costs, expenses, damages, claims and settlement amounts arising out of or relating to any reliance by a Relying Party on any Buypass Class 2 Merchant Certificate or any service provided in respect to Buypass Class 2 Merchant Certificates for:

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

The applicable Subscriber Agreement MAY include additional indemnity obligations.

2.3.2 Fiduciary relationships

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

2.3.3 Administrative processes

No stipulations.

2.4 Interpretation and enforcement

2.4.1 Governing law

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

2.4.2 Severability, survival, merger, notice

Severability
In the event that a clause or provision of the Certificate Policy for Buypass Class 2 Merchant Certificates [14] or the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] is held to be unenforceable by a court of law, the remainder of the respective Certificate Policy or Certification Practice Statement SHALL remain valid.

Survival
Subscribers and Relying Parties SHALL be bound by its terms for all Buypass Class 2 Merchant Certificates issued for the remainder of the validity periods of such Certificates, also upon termination or expiration of the Certificate Policy for Buypass Class 2 Merchant Certificates [14], the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] or any Subscription Agreement.

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

Notice

Any notice to be given by a Subscriber, Applicant, or Relying Party to Buypass under the Certificate Policy for Buypass Class 2 Merchant Certificates [14], the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19] or a Subscription Agreement SHALL be given in writing (e-mail, facsimile, post, courier) to the contact point specified in section 1.4.

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

2.4.3 Dispute resolution procedures

Any dispute arising out of or in respect to any Buypass Class 2 Merchant Certificate or any services provided in respect to any Buypass Class 2 Merchant Certificate that is not resolved by alternative dispute resolution SHALL be brought to a Norwegian court for settlement. Oslo District Court SHALL be the exclusive first instance venue for all such disputes.

2.5 Fees

No stipulation.

2.6 Publication and repositories

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

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

2.7 Compliance audit

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

2.8 Confidentiality policy

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

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

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

2.9 Intellectual property right

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

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

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

d) Buypass SHALL retain all Intellectual Property Rights in and to the Certificate Policy for Buypass Class 2 Merchant Certificates [14] as well as the Certification Practice Statement for Buypass Class 2 Merchant Certificates [19].

3 Identification and authentication

3.1 Initial registration

3.1.1 Identification/authentication of Subscriber and Subscriber Representatives

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

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

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

3.1.2 Authorization of Subscriber Representatives

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

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

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

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

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

3.2 Certificate Rekey

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

3.3 Revocation requests

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

4 Operational requirements

4.1 Certificate Application

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

4.1.1 Initial application

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

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

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

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

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

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

4.1.2 Rekey application

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

4.2 Certificate issuance

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

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

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

c) If the CA generates the Subject's key pair:
- the procedure of issuing the Certificate SHALL be securely linked to the generation of the key pair by the CA;
- the Private Key SHALL be securely passed to the registered Subject Sponsor;

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

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

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

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

4.3 Certificate acceptance

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

4.4 Certificate suspension and revocation

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

a) The CA SHALL offer a revocation management service. Revocations requests may be submitted 24x7.

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

c) Revocation status information SHALL be available 24x7. Upon system failure, service or other factors which are not under the control of the CA, the CA SHALL make best endeavors to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement.

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

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

4.4.1 Circumstances for revocation

A Certificate SHALL be revoked if:

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

- the CA determines that any of the information appearing in the Certificate is inaccurate or misleading
- the CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate
- the Private Key of the Subordinate CA used for issuing that Certificate is suspected to have been compromised
- the Subscriber ceases to exist
- the Merchant Agreement is terminated

4.4.2 Who can request revocation?

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

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

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

4.4.3 Procedure for revocation request

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

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.

4.4.4 Revocation request grace period

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

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

4.4.5 Circumstances for suspension

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

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

4.4.6 Who can request suspension

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

4.4.7 Procedure for suspension request

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

4.4.8 Limits on suspension period

a) A Certificate that has been suspended SHALL be revoked or unsuspended at the latest 30 days CRL issuance frequency

a) The CA SHALL provide a CRL service.

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

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

4.4.9 CRL checking requirements

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

4.4.10 On-line revocation/status checking availability

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

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

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

4.4.11 On-line revocation checking requirements

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

4.4.12 Other forms of revocation advertisements available

No stipulations.

4.4.13 Checking requirements for other forms of revocation advertisement

No stipulations.

4.4.14 Special requirements regarding key compromise

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

4.5 Security audit procedures

4.5.1 Types of events recorded

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

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

b) The foregoing record requirements include, but are not limited to, an obligation to record the following events:
- CA key lifecycle management events, including:
  - key generation, backup, storage, recovery, archival, and destruction
  - cryptographic device lifecycle management events
- CA and Certificate lifecycle management events, including:

- Certificate Applications, rekey applications and revocation
- all verification activities required
- date, time, phone number used, persons spoken to, and end results of verification telephone calls
- acceptance and rejection of Certificate Applications
- issuance of Certificates
- generation of Certificate Revocation Lists (CRLs) and OCSP entries

- security events, including:
  - successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed
  - security profile changes
  - system crashes, hardware failures, and other anomalies
  - firewall and router activities
  - entries to and exits from the CA facility

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

4.5.2 Frequency of processing log

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

b) Other audit logs SHALL be processed as needed.

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

4.5.3 Retention period for audit log

See section 4.6

4.5.4 Protection of audit log

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

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.

4.5.5 Audit log backup procedures

There SHALL be offsite backup of all audit logs.

4.5.6 Audit collection system

No stipulations.

4.5.7 Notification to event causing subject

No stipulations.

4.5.8 Vulnerability assessment

No stipulations.

4.6 Records archival

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

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

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

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

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

4.7 Key changeover

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

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

4.8 Compromise and disaster recovery

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

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

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

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

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

e) In the case of a CA key compromise the CA SHALL as a minimum provide the following undertakings:

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

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

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

4.9 CA termination

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

a) Before the CA terminates its services the CA SHALL execute the following procedures as a minimum:
- inform the following of the termination: all Subscribers, Relying Parties and other entities with which the CA has agreements or other form of established relations. In addition, this information shall be made available to other Relying Parties
- terminate all authorization of Subcontractors to act on behalf of the CA in the performance of any functions related to the process of issuing Certificates
- perform necessary undertakings to transfer obligations for maintaining registration information, revocation status information and event log archives for their respective period of time as indicated to the Subscriber and Relying Party
- destroy or put beyond use all copies of the CA private signing keys
- revoke unexpired unrevoked Subscriber Certificates, if required

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

5 Physical, procedural, and personnel security controls

5.1 Physical security controls

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

b) Any persons entering this physically secure area SHALL NOT be left for any significant period without oversight by an authorized person.

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.

d) Physical and environmental security controls SHALL be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The CA's physical and environmental security policy for systems concerned with Certificate generation, Subject key generation, Subject key provision and revocation management services shall address the physical access control, natural disaster protection, fire safety factors,

failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc.

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

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

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

5.2 Procedural controls

5.2.1 Trusted roles

a) All personnel engaged in CA related tasks are considered trusted personnel. The following trusted roles are defined:
- **Security Manager:** is overall responsible for security and formally appoints personnel to the other trusted roles
- **Security Officer:** is responsible for the implementation of the security practices
- **Security Auditor:** is responsible for controlling that routines are complied with and for reading and maintaining archives and audit logs
- **System Administrator:** is responsible for the operation of the system and installing security software and hardware

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

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.

5.2.2 Number of persons required per task

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

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

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

5.2.3 Identification and authentication for each role

No stipulations.

5.3 Personnel security controls

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

5.3.1 Background, qualifications, experience, and clearance requirements

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

b) 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.

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

5.3.2 Background check procedures

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

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.

5.3.3 Retraining frequency and requirements

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

5.3.4 Job rotation frequency and sequence

No stipulations.

5.3.5 Sanctions for unauthorized actions

a) Appropriate disciplinary sanctions SHALL be applied to personnel violating the Certificate Policy for Buypass Class 2 Merchant Certificates [14] or underlying operative procedures.

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

5.3.6 Contracting personnel requirements

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

5.3.7 Documentation supplied to personnel

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

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

CA key generation

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

b) The CA private signing key SHALL be generated within a cryptographic device which either:
- meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3] level 3 or higher

- meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [10], CWA 14167-3 [11] or CWA 14167-4 [12]
- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [13] or equivalent security criteria

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

Subject key generation performed by the CA

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

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

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

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

Subject key generation performed by the Subscriber

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

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

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

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

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

6.1.2 Private Key delivery to entity

For CA generated private Subject keys the following requirements apply:

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

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

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

6.1.3 Public Key delivery to Certificate issuer

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

- authenticate the Subscriber or Subject Sponsor as the originator of the request

- contain proof that the requestor is in possession of the Private Key that corresponds to the Public Key in the request

6.1.4 CA Public Key delivery to users

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

6.1.5 Key sizes

CA keys

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

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

Subject keys

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

6.1.6 Public Key parameter generation

No stipulations.

6.1.7 Parameter quality checking

No stipulations.

6.1.8 Hardware/software key generation

See 6.1.1

6.1.9 Key usage

CA keys

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

Subject keys

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

6.2 Private Key protection

6.2.1 Standards for cryptographic module

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

a) The CA private signing key SHALL be held and used within a secure cryptographic device which meets the requirements as defined in 6.1.1 b).

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

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.

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

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

6.2.2 Private Key (n out of m) multi-person control

See 6.1.1, 6.2.4 and 6.2.7

6.2.3 Private Key escrow

No stipulations.

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.

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

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

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.

6.2.5 Private Key archival

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

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

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

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

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

6.2.6 Private Key entry into cryptographic module

See 6.1.1 and 6.2.4

6.2.7 Method of activating Private Key

CA Private Key

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

Subject Private Key

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

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

6.2.8 Method of deactivating Private Key

No stipulations.

6.2.9 Method of destroying Private Key

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

No stipulations for Subject Private Keys.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulations.

6.3.2 Usage periods for the Public and Private Keys

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

CA keys

a) The CA SHALL ensure that CA private signing keys are not used beyond the end of their life cycle.

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

Subject keys

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

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

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.

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

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

6.4.2 Activation Data protection

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

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

6.4.3 Other aspects of Activation Data

No stipulations.

6.5 Computer security controls

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

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

6.6 Life cycle technical controls

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

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

6.7 Network security controls

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

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

6.8 Cryptographic module engineering controls

No stipulations.

7 Certificate and CRL profiles

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

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

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

8 Specification administration

8.1 Specification change procedures

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

8.2 Publication and notification procedures

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

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

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

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

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

8.3 CPS approval procedures

No stipulations.