Version: 4.2
Date: 02.05.2024

MAIN PART OF THE SUBSCRIBER AGREEMENT (PART 1)

1 Introduction

This document (Part 1), along with the Registration Form (Part 2), the Application Form for Buypass Class 3 SSL Certificates (Part 3) and the *Certification Practice Statement for Buypass Class 3 SSL Certificates* (Part 4) constitutes the Subscriber Agreement for Buypass Class 3 SSL Certificates. The Registration Form and the Application Form can be combined to make a joint Registration and Application Form which would then constitute both Parts 2 and 3 of the agreement.

Buypass Class 3 SSL Certificates includes SSL Business Plus, SSL Evident (EV) and Qualified Website Authentication Certificates (SSL QWAC and SSL QWAC for PSD2).

For Qualified Website Authentication Certificates the *PKI Disclosure Statement* (Part 5) also constitutes a part of the Subscriber Agreement.

Please refer to the other documents for the technical specifications and details of the SSL certificate's features. For further information please refer to Buypass Web.

This document (the main part of the Subscriber Agreement) constitutes Part 1 of the Subscriber Agreement between the Subscriber and Buypass.

The Registration Form (Part 2) contains subscriber-specific agreement information and a signature. The Application Form (Part 3) contains certificate-specific agreement information. The Registration and Application Form contain both subscriber-specific and certificate-specific agreement information.

The terms and conditions contained in this document (Part 1) shall apply unless exceptions to one or more of the terms and conditions have been made in the Registration Form (Part 2).

The Subscriber may enter into more than one agreement with Buypass for SSL certificates.

The Subscriber may authorise natural persons and/or Partners to apply for, approve, manage and use SSL certificates on behalf of the Subscriber. The roles which can be assigned to natural persons by the Subscriber are hereafter referred to as Contract Signer, Authorized Officer, Certificate Manager, Certificate Approver and Certificate Applicant. The Certificate Approver role may be assigned to a Partner.

These authorisations must be stated on the Registration Form (Part 2) and may apply to all future applications until authorisation is withdrawn if this is specified in the Registration Form.

Buypass shall deal with the Subscriber as a contractual party, and the Subscriber shall be responsible for any actions carried out by the Subscriber's Certificate Managers, Certificate Approvers and Certificate Applicants.

2 Definitions

Term	Abbreviation	Description
Application Form (Part 3 of the Subscriber Agreement)		The Application Form contains certificate-specific information and is conditional on the Registration Form (Part 2).

Term	Abbreviation	Description
Authorization Number		A unique identifier of a Payment Service Provider acting as the Subscriber for PSD2 Certificates. The Authorization Number is used and recognized by the NCA.
Authorized Officer		Authorized Subscriber Representative who has authority on behalf of Subscriber to confirm the identity of the Subscriber by physical presence according to article 24 of the Regulation (EU) No 910/2014. The Contract Signer may act as Authorized Officer.
Authorized Subscriber Representatives		Natural persons assigned the roles Certificate Manager, Certificate Approver and Certificate Applicant and/or Partners assigned the role Certificate Approver.
Buypass Web		Websites operated by Buypass, i.e. www.buypass.no and www.buypass.com.
Certificate Applicant		Authorized Subscriber Representative who has authority to submit a Certificate Application on behalf of the Subscriber.
Certificate Approver		Authorized Subscriber Representative who has authority to (i) act as a Certificate Applicant and to authorize other employees or third parties to act as a Certificate Applicant, and (ii) to approve Certificate Applications submitted by Certificate Applicants.
Central Coordinating Register for Legal Entities		Norwegian national register containing basic data (e.g. Organization name and Organization Number) about legal persons to coordinate information on business and industry that resides in various public registers ('Enhetsregisteret').
Certificate Manager		Authorized Subscriber Representative who has the authority to (i) act as a Certificate Approver and Certificate Applicant and (ii) to authorize other employees or third parties to act as a Certificate Approver or Certificate Applicant.
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.
Certification Practice Statement	CPS	Statement of the practices which a Certificate Authority employs in issuing Certificates (Part 4 of the Subscriber Agreement)
Certificate Signing Request	CSR	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 formatted request that is submitted by a Subscriber as part of a Certificate Application.
Certificate Transparency	CT	Certificate Transparency is about transparency and accountability and all SSL certificates are published in open and publicly available logs (CT logs). This makes it possible to monitor all SSL certificates issued.
CT-log		An open and publicly available log containing certificates and a component in the Certificate Transparency framework.
Contract Signer		Authorized Subscriber Representative who has authority on behalf of Subscriber to sign Subscriber Agreements.
European Business Register	EBR	The European Business Register is a network of National Business Registers and Information Providers in European Countries containing basic data (e.g. Organization name and Organization Number) about legal persons operating in these countries. EBR includes the

Term	Abbreviation	Description
		Norwegian Central Coordinating Register for Legal Entities ("Enhetsregisteret").
National Competent Authority	NCA	A national authority responsible for payment services. The NCA approves or rejects authorizations for Payment Service Providers in its country.
Organization		The legal person acting as the Subscriber
Organization's Authorized Representative		See Authorized Officer
Organization Number		Unique registration number identifying a legal person. Assigned by a national authority in the jurisdiction where the legal person operates.
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. The Partner's role is regulated by the Registration Form (Part 2).
PKI Disclosure Statement	PDS	A document that supplements a CPS by disclosing important information about the policies and practices of a CA. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CPS documents. For Qualified Website Authentication Certificates the PDS constitutes Part 5 of the Subscriber Agreement.
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. For an SSL certificate the private key is used by a server available at the domain name included in the certificate.
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. The public key is a part of the SSL certificate defining a link between the Subscriber, the specified domains and the corresponding private key.
PSD2 Certificate	PSD2 QWAC	A Qualified Website Authentication Certificate meeting regulatory requirements for PSD2 and the Regulatory Technical Standard.
Payment Service Provider	PSP	An organization authorized to provide payment services to customers.
Registration and Application Form (Parts 2 and 3 of the Subscriber Agreement)		A form which contains both general information about the Organization (subscriber-specific information) and application specific information.
Registration Form (Part 2 of the Subscriber Agreement)		A form which contains general information about the Organization, including authorisations for the Authorised Subscriber Representatives.

Term	Abbreviation	Description
Revocation		Revocation of an SSL certificate during its lifetime, i.e. when the SSL certificate is no longer valid for some reason and must no longer be used.
SSL certificate or Buypass Class 3 SSL 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. A SSL Certificate may also be issued as a Qualified Website Authentication Certificate.
Qualified Certificate	QC	See Qualified Website Authentication Certificate
Qualified Government Register	QGR	Any Authoritative Source provided by a Government Entity containing basic information about legal persons operating in the Government's jurisdiction. The basic information includes the full name of the legal person, an Organization Number and a business and/or postal address for the legal person. All registers in EBR are QGRs. QGRs hold information about legal persons as required by national legislation.
Qualified Website Authentication Certificate	QWAC	An SSL Certificate that meets the requirements to Qualified Certificates for website authentication according to the eIDAS regulation (Regulation (EU) no 910/2014).
Subscriber		An Organization to whom an SSL certificate has been issued by Buypass and who is authorised to use the private key corresponding to the SSL certificate.

3 Agreement process

Subscribers must apply for SSL certificates online on Buypass web or by alternative means as specified by Buypass.

The Registration Form (Part 2) is generated during the registration process before the Application Form (Part 3) is generated during the application process. The Registration Form must be signed by the Contract Signer. If authority is delegated to a Partner, this must be stated on the Registration Form (Part 2). When the Subscriber has previously filled in and sent the Registration Form (Part 2) to Buypass, a signature from the Certificate Manager, Certificate Approver or Certificate Applicant on an Application Form (Part 3) is sufficient for applying for SSL certificates.

A combined Registration and Application Form is generated when the application is placed, and must be signed by the Contract Signer. All subsequent applications require a signed Registration and Application Form.

Signed forms must be sent to Buypass by post or e-mail to the contact specified on the forms.

In order to comply with Buypass' security requirements on issuing SSL certificates, whoever signs the Registration Form on behalf of the Subscriber (Contract Signer) must be authorised to sign agreements/contracts on behalf of the Subscriber.

The Contract Signer may authorise a natural person to appoint Certificate Approvers and Certificate Applicants and to apply for and approve the application of SSL certificates (Certificate Manager). Such authorisations shall be given on the Registration Form (Part 2). Authorisation shall apply until it is withdrawn, cf. Item 6.

The Contract Signer or the Certificate Manager may authorise a natural person or a Partner to appoint Certificate Applicants and to apply for and approve the application of SSL certificates (Certificate Approver). Such authorisations shall be given on the Registration Form (Part 2). Authorisation shall apply until it is withdrawn, cf. Item 6.

The Contract Signer, the Certificate Manager or the Certificate Approver may authorise a natural person to apply for SSL certificates (Certificate Applicant). Such authorisations shall be given on the Registration Form. Authorisation shall apply until it is withdrawn if this is specified in the Registration Form, cf. Item 6.

For Qualified Website Authentication Certificates, the Subscriber authorizes a natural person to confirm the identity of the Subscriber by physical through the Subscriber Agreement (Authorized Officer). This authorization may also be granted the Certificate Approver.

Buypass will verify the contents upon receipt of the Registration Form, the Application Form and the Registration and Application Form. The verifications are described in Part 4 of the Subscriber Agreement.

The Subscriber shall inform the Authorised Subscriber Representatives about obligations incurred by the Subscriber under the Subscriber Agreement.

Buypass publishes all SSL certificates in 2 or 3 CT logs dependent of the certificate validity period. By accepting the Subscriber Agreement, the Subscriber agrees to such publication of the SSL certificate.

4 The Subscriber's responsibilities and rights

4.1 Introduction

SSL certificates are inseparably linked to the Organization (Subscriber) and the specified domain(s). The Subscriber is responsible for ensuring that SSL certificates are not misused by the Subscriber's representatives. The Subscriber is also responsible for ensuring that SSL certificates are used in accordance with current legislation and the terms and conditions contained in this document.

The Subscriber is responsible for using the SSL certificate only for the purposes stated in this agreement.

4.2 Registration of the Subscriber

The Subscriber shall undertake to provide complete and correct information upon registration. This shall also apply when Buypass requests additional information or documentation during validation of the registered information.

The Subscriber is responsible for maintaining Authorized Subscriber Representatives at all times, i.e. Authorized Subscriber Representatives who are no longer authorized must be withdrawn. The Subscriber must ensure that Authorized Subscriber Representatives maintain their contact information at all times so that they can receive notifications and act upon them immediately.

For QWACs, the Subscriber designates the Authorized Officer to confirm the identity of the Subscriber by physical presence or by using methods which provide equivalent assurance in terms of reliability to physical presence. The Subscriber must ensure that the Authorised Officer is authorised according to the requirements in the eIDAS regulation (Regulation (EU) no 910/2014).

For PSD2 QWACs, the Subscriber must have been granted the authorization to act as a PSP in the ‘applied for’ PSP roles by a National Competent Authority (NCA) in the country the Subscriber operates as a PSP according to the PSD2 legislations. If the Subscriber is assigned a specific Authorization Number by the NCA, this must be specified at time of registration and application.

The Subscriber shall undertake to inform Buypass immediately if the information provided is no longer correct.

4.3 Applying for SSL certificates

Prior to applying the Subscriber will need to have the private and public key generated. The public key is included in the application. The Subscriber shall undertake to keep and protect the private key in a suitable manner at all times.

The Subscriber shall also undertake to provide complete and correct information in the application. This shall also apply when Buypass requests additional information or documentation during validation of the application.

The Subscriber shall undertake to inform Buypass immediately if the information provided is no longer correct.

4.4 Installation and use of SSL certificates by the Subscriber

The Subscriber shall verify that the contents in the SSL certificate are correct prior to installation and use. The Subscriber must notify Buypass immediately if there are any errors in the contents. The contents in the SSL certificate are accepted upon installation. Regardless of this the Subscriber must notify Buypass if any errors in the contents are detected after installation.

Unless the Subscriber has reported errors in the contents, Buypass consider the SSL certificate to be accepted 14 days after the issuance date.

SSL certificates issued under this agreement may only be installed on servers which are available on the same domain name(s) as specified in the SSL certificate. The SSL certificate should not be installed on equipment which is not under the control of the Subscriber.

The Subscriber shall be fully liable for ensuring that the SSL certificate is installed and protected so that only the Subscriber's representatives can manage the private key and the SSL certificate. The Subscriber shall implement reasonable measures to prevent any unauthorised use of the private key.

4.5 Revoking SSL certificates

If the Subscriber knows, or has reason to believe, or should have understood that any unauthorised persons have acquired knowledge about the private key, the Subscriber shall immediately take steps to revoke the SSL certificate. The SSL certificate shall be revoked in the event of loss, misuse or suspected misuse. Failure to do so shall be regarded as coarse negligence. The SSL certificate shall also be revoked if the information in the certificate is incorrect or inaccurate.

If the SSL certificate is revoked due to one of the reasons listed below (read about revocation reasons on Buypass Web), the reason must be specified when requesting revocation:

- the private key is compromised (keyCompromize #1)
- the Subscriber’s name or other identity information in the certificate has changed (affiliationChanged #3)
- the certificate has been replaced by another certificate (superseded #4)
- the certificate contains domain names that are no longer in use or the certificate will no longer be used because the website is no longer operative (cessationOfOperation #5)

A reason code (in parentheses) will be included on the CRL/OCSP giving information to relaying parties about the reason for revoking the certificate. If the certificate is revoked for any other reason, no reason code should be specified.

For PSD2 QWACs, the certificate shall be revoked if the authorization to act as a PSP has been withdrawn, or any of the PSP roles included in the certificate has been withdrawn.

Subscribers may submit revocation requests to Buypass’ revocation service by phone or by contacting the revocation service on Buypass Web. The Contract Signer and Authorized Subscriber Representatives may request certificate revocation on behalf of the Subscriber.

The Subscriber must ensure that Authorized Subscriber Representatives are, at any time, able to receive and acknowledge notifications from Buypass regarding any incident that requires certificates to be revoked within 24 hours or 5 days depending on the severity of the incident, and act upon them immediately. In such cases the Subscriber is responsible for replacing affected SSL certificates within the given timeframe to avoid services becoming inaccessible when certificates are revoked.

The Subscriber shall stop using the private key immediately when:

- the information in the SSL certificate is incorrect or invalid
- it is suspected or demonstrated that the private key has been subject to misuse or has been compromised
- the SSL certificate has been revoked

If it is suspected or demonstrated that the private key has been subject to misuse or has been compromised, the Subscriber shall immediately comply with Buypass' instructions on the use of private keys and SSL certificates.

The loss of a private key implies that the Subscriber must apply for a new SSL certificate.

5 Buypass' responsibilities and rights

5.1 Processing of Subscriber information and personal data

5.1.1 Collection and storage

As part of the Subscriber registration, Buypass will collect and store personal data about Subscriber's representatives.

If Buypass at some point chooses to terminate the service covered by this agreement, the personal data for Subscribers with active certificates may be transferred to a third party who assumes responsibility for the continuation of the service until the certificates expire. In this case, Buypass will notify the Subscriber and retrieve the Subscriber's consent to this transferal of data.

5.1.2 Purpose

This information will not be used without the Subscriber's consent for any other than necessary communication or production of services under this Subscriber Agreement. The information will be deleted as soon as the agreement is no longer applicable unless continued retention is required by law.

5.1.3 Consent

By accepting the Subscriber Agreement, the Subscriber agrees that Buypass may process Subscriber's information and Subscriber representatives' personal data as described in this Agreement.

5.1.4 Right to access, change and delete

Buypass is responsible for the handling of this data and the Subscriber may ask questions relating to the processing of personal data to Buypass Customer Support.

The Subscriber and the Subscriber representatives also have the right to require access to and possible correction of personal data that is registered in connection with the Subscriber.

The Subscriber also has the right to require that personal data about certain Subscriber's representatives be deleted, unless continued retention is required by law.

5.1.5 Information security

Buypass is responsible for the protection of personal data and shall, through planned and systematic measures, ensure that adequate information security is in accordance with the laws in force at any time.

Buypass has confidentiality in relation to the registered personal data and will not disclose it to third parties, unless such disclosure is required by lawful judgment, applicable law, or according to the Subscriber's written request or requirement.

5.2 Buypass' liability

Buypass' entire liability for damages relating to the use of SSL certificates issued by Buypass is set out in the CPS in force from time to time for Buypass Class 3 SSL Certificates (Part 4 of the Subscriber Agreement). Buypass shall have no additional liability under this Subscriber Agreement.

5.3 Revoking SSL certificates

Buypass may revoke an SSL certificate if the Subscriber fails to comply with the terms and conditions contained in this agreement or if the certificate is used for illegal activities such as phishing or fraud or is otherwise misused.

Buypass may also revoke an SSL certificate if Buypass is made aware that important information in the certificate is incorrect or inaccurate or the Subscriber no longer exists.

Buypass may, at any time, notify the Subscriber via Authorized Subscriber Representatives about incidents that require SSL certificates to be revoked, and revoke any SSL certificate within 24 hours or 5 days depending on the severity of the incident. Incidents that require revocation may be changes in requirements, compromised keys or compromised algorithms etc.

If the certificate is revoked for any reasons listed below, the reason will be specified when revoking the certificate and included as reason code on CRL and OCSP (see also 4.5):

- Buypass obtains evidence that the private key has been compromised (keyCompromize #1)
- Buypass is made aware that the Subscriber's name or other identity information in the certificate has changed (affiliationChanged #3)
- Buypass finds it necessary to revoke the certificate because it no longer satisfies the requirements stated in the CP/CPS (superseded #4)
- Buypass is made aware that the certificate contains domain names that are no longer allowed to use (cessationOfOperation #5)
- Buypass obtains evidence that the certificate has been misused or is made aware of that the Subscriber fails to comply with terms and conditions in this agreement (privilegeWithdrawn #9)

If the certificate is revoked for any other reason, no reason code will be specified.

Buypass may revoke PSD2 QWACs based on revocation requests from an NCA identified in the certificate in case the Subscriber (PSP) has lost its authorization to act as a PSP or any PSP role in the certificate has been withdrawn.

The Subscriber will be notified when Buypass revoke an SSL certificate.

5.4 Notification to other entities

When a PSD2 QWAC is issued, Buypass will send an issuance notification email to the NCA identified in the Certificate using pre-registered NCA contact information if such contact information has been provided by the NCA.

When a PSD2 QWAC is revoked, Buypass will send a revocation notification email to the NCA identified in the Certificate using pre-registered NCA contact information if such contact information has been provided by the NCA.

6 Amendments to the Subscriber Agreement

If the Subscriber needs to change any Subscriber-specific information in Part 2 of the Subscriber Agreement, the Subscriber shall update the information registered online at Buypass Web or by alternative means as specified by Buypass. The updated Registration Form (Part 2) shall be signed by the Contract Signer and sent to Buypass. The Registration Form (Part 2) shall be sent as specified on the form. The requirements which applied to signature of the original Registration Form shall also apply to signing the updated Registration Form, cf. Item 3.

If the Subscriber wants to assign new natural persons to the role of Certificate Manager, the Subscriber shall update the information registered as specified above. The updated Registration Form shall be signed by the Contract Signer.

If the Subscriber wants to assign new natural persons and/or Partners to the role of Certificate Approver, the Subscriber shall update the information registered as specified above. The updated Registration Form shall be signed by the Contract Signer or the Certificate Manager.

If the Subscriber wants to assign new natural persons to the role of Certificate Applicant, the Subscriber shall update the information registered as specified above. The updated Registration Form shall be signed by the Contract Signer, the Certificate Manager or the Certificate Approver.

The Subscriber shall undertake to notify Buypass when any natural person and/or Partners is no longer authorised to have the roles of Contract Signer, Certificate Manager, Certificate Approver or Certificate Applicant. Notification shall be given by updating the information registered as specified above.

7 Duration of the Subscriber Agreement

The Subscriber Agreement shall be valid for as long as the SSL certificates subject to this agreement are valid or until they are revoked. The Subscriber shall be responsible for applying for new SSL certificates before his active SSL certificates expire.

If the Subscriber defaults on his commitments under the Subscriber Agreement and fails to rectify the situation within a reasonable deadline determined by Buypass, Buypass may cancel the Subscriber Agreement with immediate effect. If default is such that it cannot be rectified, Buypass may cancel the Subscriber Agreement with immediate effect. In the event of such cancellation of the agreement, the SSL certificates subject to this agreement will be revoked.

Buypass may amend the contents of Part 4 (CPS) or the Part 5 (PDS) of the Subscriber Agreement by publishing an updated CPS or PDS on Buypass Web. The new CPS or PDS shall then apply whenever the SSL certificates are used after publication of the new CPS or PDS.

8 Legal venue and governing law

If any disagreements arise between the parties about the interpretation or legal effects of this agreement, the parties shall initially try to reach agreement amicably through negotiations and/or mediation.

If a dispute cannot be resolved through negotiations or mediation, either of the parties may submit the dispute for final resolution by the ordinary courts of Norway. Both parties submit to the exclusive jurisdiction and venue of the courts of Oslo, Norway.

This agreement, as well as the relationship between the Subscriber and Buypass, is regulated by Norwegian law, without regard to its choice of law principles.

9 Force Majeure

Should any extraordinary situation arise which is beyond the control of the parties and which makes it impossible to comply with this agreement and which under Norwegian law is regarded as being force majeure, the other contracting party shall be notified without undue delay. The obligations of the affected party shall be suspended for the duration of the extraordinary situation concerned. The other party's corresponding services shall be suspended during the same period.

10 Contact details for Buypass

Buypass AS
Post-box 4364 Nydalen
Nydalsveien 30 A
N-0402 Oslo

see Buypass Web, email:
support@buypass.com

Buypass Certificate Revocation Service:
see Buypass Web

Customer Support:
see Buypass Web, email:
support@buypass.com