Version: 5.2
Date: 01.10.2023

PUBLIC

PKI Disclosure Statement

Buypass Qualified Certificates

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

www.buypass.no | 22 70 13 00

TABLE OF CONTENTS

NOTICE

The purpose of this PKI Disclosure Statement is to summarize and present the main points from the Certificate Policies (CP) and Certification Practice Statements (CPS) for all Buypass Qualified Certificates in a more readable and understandable format for the benefit of our Subscribers and Relying Parties.

A PKI Disclosure Statement does not replace a CP or CPS which is essential documents for describing and governing certificate policies and practices.

1 Contact info

Contact information for Buypass AS as a Qualified Trust Service Provider (QTSP).

Name:	Buypass AS
Location:	Nydalsveien 30A, Oslo, Norway
Post address:	Postboks 4364 Nydalen, N-0402 Oslo
Telephone:	+ 47 22 70 13 00
Contact email:	policy@buypass.no
Website:	www.buypass.com (www.buypass.no)
Customer Support:	https://www.buypass.com/the-company/contact-customer-support (https://www.buypass.no/selskapet/kontakt-kundeservice)
Revocation Service:	https://www.buypass.com/security/revocation-service (https://www.buypass.no/sikkerhet/sperretjeneste)
Problem Reporting:	https://www.buypass.com/ssl-support/ssl-problem-reporting (https://www.buypass.no/ssl-support/ssl-problemrapportering)

2 Certificate type, validation procedures and usage

This statement applies to Qualified Certificates issued by Buypass AS. Buypass Qualified Certificates are issued as Buypass Class 3 certificates and they are EU Qualified Certificates according to Regulation (EU) No 910/2014.

Buypass Qualified Certificates also includes PSD2 Certificates that meet the Regulatory Technical Standard Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

Buypass Qualified Certificates must not be used for any other purpose than specified below. Specifically, the certificates must not be used to sign software, certificates and/or revocation lists.

Buypass Qualified Certificates for electronic signatures are issued to natural persons registered in the National Population Register. The identity of the natural person is verified by physical presence of the natural person.

The private keys corresponding to these Qualified Certificates should only be used for electronic signatures.

These Qualified Certificates must not be used as a basis for issuing other certificates, electronic IDs or credentials unless explicitly agreed upon by Buypass.

The Certificate Policy for these certificates is Buypass Class 3 Qualified Certificates for electronic signatures and the certificates have been provided the following Certificate Policy Identifiers/OIDs:

- OID=2.16.578.1.26.1.3.1 – the private keys are protected in a smart card
- OID=2.16.578.1.26.1.3.6 – the private keys are protected in an HSM

Buypass Cloud Signature Services (BCSS) Qualified Certificates for electronic signatures are issued to natural persons based on an authentication using an already existing eID means. The identity of the natural person is verified by using the eID means that must comply with eIDAS art 24 1 b) in terms of equivalence with physical presence of the natural person and meet the requirements for eID level of assurance (LoA) High or Substantial.

The private keys corresponding to these Qualified Certificates will only be used for qualified electronic signatures.

These Qualified Certificates must not be used as a basis for issuing other certificates, electronic IDs or credentials unless explicitly agreed upon by Buypass.

The Certificate Policy for these certificates is Buypass Class 3 BCSS Person Certificates and the certificates have been provided the following Certificate Policy Identifiers/OIDs:

- OID 2.16.578.1.26.1.3.8 (Buypass OID)
- OID 0.4.0.194112.1.2 (ETSI QCP-n-qscd)

These certificates are short-term certificates with a validity period of hours certifying a one-time private key generated and used within a QCSD as a part of the BCSS Person Signing Service.

Buypass Qualified Certificates for electronic Seals are issued to legal persons registered in the European Business Register or other generally recognized dependable information sources. The identity of the legal person is verified by physical presence of an authorized representative of the legal person or by using methods which provide equivalent assurance in terms of reliability to physical presence.

The private keys corresponding to these Qualified Certificates should only be used for electronic seals.

These Qualified Certificates must not be used as a basis for issuing other certificates, electronic IDs or credentials unless explicitly agreed upon by Buypass. The Certificates must not be used for web-based data communication conduits via the TLS-protocol.

The Certificate Policy for these certificates is Buypass Class 3 Enterprise Certificates and the certificates have been provided the following Certificate Policy Identifiers/OIDs:

- OID 2.16.578.1.26.1.3.2 – provided as Soft Token
- OID 2.16.578.1.26.1.3.5 – provided as Hard Token

Buypass Qualified Certificates for electronic Seals also include one of the following OIDs:

- OID 0.4.0.194112.1.1 (ETSI QCP-l)
- OID 0.4.0.194112.1.3 (ETSI QCP-l-qscd)

These Qualified Certificates may also be issued to legal persons where the private key and the related certificate reside on a Hard Token certified as a Qualified Seal Creation Device (QCP-l-qscd).

Buypass Qualified Certificates for electronic Seals may also be issued as PSD2 Certificates.

Buypass Qualified Website Authentication Certificates are issued to legal persons registered in the European Business Register or other generally recognized dependable information sources. The identity of the legal person is verified by physical presence of an authorized representative of the legal person or by using methods which provide equivalent assurance in terms of reliability to physical presence.

The legal person must either be a Private Organization, a Business Entity or a Government Entity according to the definitions in the CA/Browser Forum EV Guidelines.

The validation procedures for these certificates are compliant to validation procedures for Extended Validation certificates according to the CA/Browser Forum EV Guidelines.

The private keys corresponding to these Qualified Certificates should only be used for authentication in the TLS-protocol.

The Certificate Policy for these certificates is Buypass Class 3 SSL Certificates and the certificates have been provided the following Certificate Policy Identifiers/OIDs:

- OID 2.16.578.1.26.1.3.3 - Buypass SSL Evident Certificates
- OID 2.23.140.1.1 – CABF EV OID

Buypass Qualified Website Authentication Certificates must not necessarily be accepted as TLS certificates by browsers and for this purpose we have assigned a separate OID which may be used instead of the two OIDs defined above:

- OID 2.16.578.1.26.1.3.7 - Buypass Qualified Website Authentication Certificate

Buypass Qualified Website Authentication Certificates also includes the following OID

- OID 0.4.0.194112.1.4 (ETSI QEVCP-w)

Buypass Qualified Website Authentication Certificates may also be issued as PSD2 Certificates using the following OID:

- OID 0.4.0.19495.3.1 (ETSI QCP-w-psd2)

3 Reliance limits

Registration information and event logs are retained for at least 7 years after any certificate based on these records ceases to be valid.

Buypass Qualified Certificates for electronic signatures are only to be used for electronic signatures according to the Regulation (EU) No 910/2014.

BCSS Qualified Certificates for electronic signatures are short-term certificates only to be used for qualified electronic signatures in the BCSS Person Signing Service according to the Regulation (EU) No 910/2014.

Buypass Qualified Certificates for electronic Seals are only to be used for electronic seals according to the Regulation (EU) No 910/2014.

Buypass Qualified Website Authentication Certificates are only to be used for website authentication according to the Regulation (EU) No 910/2014.

4 Obligations of subscribers

For all Buypass Qualified Certificates, the Subscriber is obliged to:

- Fulfill all the obligations of the Subscriber Agreement
- Submit accurate and complete information when applying for certificates
- Exercise reasonable care to avoid unauthorized use of the Subjects Private Keys
- Be responsible for ensuring that restrictions on Private Keys and certificates use are maintained
- Ensure that restrictions on the use of Private Keys and certificates are maintained
- Notify the TSP if any information in the certificate is incorrect
- Request the certificate to be revoked when a valid revocation reason exists
- Ensure that the Private Key is no longer used in the case of Private Key compromise, i.e. the control over Subject Private Key is lost
- Ensure that the Private Key is no longer used in the case of being informed that the CA has been compromised

In addition, for Buypass Qualified Certificates for electronic Seals the Subscriber is obliged to:

- Ensure that the use of the certificate is under Subscriber control by recording all entities that have access to and use the private keys, this includes individuals, systems and processes
- Ensure that the private keys are used for electronic Seal only

In addition, for Buypass Qualified Website Authentication Certificates the Subscriber is obliged to:

- Install the certificate only on the server accessible at the domain name listed in the certificate
- Not install or use the certificate until it has been reviewed and the accuracy of the data in the certificate has been verified

5 Certificate status checking obligations of relying parties

In order to reasonably rely on a Buypass Qualified Certificate, a Relaying Party must verify that the certificate is used in accordance with its defined purpose.

A Relying Party must also check the validity of the certificate.

The Relying Party is obliged to

- Verify that the digital signature has been generated with a private key that corresponds to the public key in the certificate
- Verify that the certificate was valid at time of using the private key, i.e. the time must be before the valid until in the certificate
- Verify that the certificate was not revoked at time of using the private key, i.e. the revocation status must be checked either using OCSP or CRL as indicated in the certificate
- Verify all certificates in the certificate path according to best practice as defined by RFC 5280

The BCSS Qualified Certificates for electronic signatures are short-term certificates without support for revocation. However, a CRL-service is available in case such evidence should be required.

6 Limited warranty and disclaimer/Limitation of liability

Limitations of liability are according to Norwegian law. Relying Parties and Subscribers can buy into coverage schemes that will improve Relying Party protection.

Buypass has defined the following yearly liability caps for **Buypass Qualified Certificates for electronic signatures:**

- 10.000 NOK (ten thousand Norwegian Kroner) per Subscriber or Relying Party concerning a specific certificate or any services provided in respect to this certificate. The total liability for damages for a specific Relaying Party concerning all certificates or any services in respect to these certificates is limited to 50.000 NOK (fifty thousand Norwegian Kroner).

Buypass has defined the following liability limitations for **BCSS Qualified Certificates for electronic signatures:**

- The total liability for damages for a specific Relaying Party concerning all certificates or any services in respect to these certificates is limited to 200.000 NOK (two hundred thousand Norwegian Kroner).

Buypass has defined the following yearly liability caps for **Buypass Qualified Certificates for electronic Seals:**

- 2.000 EUR (two thousand Euros) per Subscriber or Relying Party concerning a specific certificate or any services provided in respect to this certificate.

Buypass has defined the following yearly liability caps for **Buypass Qualified Website Authentication Certificates:**

- 2.000 USD (two thousand United States Dollars) per Subscriber or Relying Party concerning a specific certificate or any services provided in respect to this certificate.

Buypass maintains insurances to protect its service related to **Buypass Qualified Website Authentication Certificates**.

7 Applicable agreements, CPS, CP

Applicable agreements, CP and CPS documents are publicly available at
https://www.buypass.com/support/download-center#ca-documentation
(https://www.buypass.no/sikkerhet/ca-dokumentasjon-juridisk)

For Buypass Qualified Certificates for electronic Signatures, see
Buypass Class 3 Person Qualified Certificates (Personlige kvalifiserte sertifikater).

For BCSS Qualified Certificates for electronic Signatures, see
BCSS Person Signing (BCSS Personsignatur).

For Buypass Qualified Certificates for electronic Seals, see
Buypass Class 3 Enterprise Certificates (Buypass Class 3 Virksomhetssertifikater).

For Buypass Qualified Website Authentication Certificates, see
Buypass Class 3 SSL Certificates (Buypass Class 3 SSL-sertifikater).

8 Privacy policy

Subscriber information is processed in accordance with applicable legislation for personal data protection according to in Norwegian law.

9 Refund policy

Buypass' refund policy is in accordance with applicable legislation in Norwegian law.

10 Applicable law, complaints and dispute resolution

Complaints from customers or other parties related to Buypass Qualified Certificates or any services provided in respect to these certificates will be handled without any unreasonable delay and the complaining party will receive an answer to the complaint within 14 calendar days from the reception of the complaint.

In case of a dispute arising the parties shall try to settle the dispute through negotiations and conciliation.

If the dispute is not resolved within 3 months from the commencement of the conciliatory process, each party has the right to bring the dispute to a Norwegian court for settlement. Oslo District Court will be the exclusive first instance venue for all such disputes.

11 TSP and repository licenses, trust marks, and audit

Buypass is a Qualified Trust Service Provider (QTSP) and issues Qualified Certificates according to Regulation (EU) No 910/2014.

Buypass is registered as a QTSP on the Norwegian Trusted List (TL) available at:
https://www.nkom.no/internett/elektronisk-id-og-tillitstjenester/tillitsliste-trusted-list

Buypass Qualified Certificates for electronic signatures complies with the requirements for the eIDAS high in 'Selvdeklarasjonsforskriften' as defined in Norwegian legislation.

Buypass is annually audited for compliance with the requirements for Qualified Certificates from ETSI EN 319 411-2, ETSI EN 319 411-1 and ETSI EN 319 401. The audit is performed by BSI Group.