buypass™

MAIN PART OF THE TERMS OF SERVICE (PART 1)

1 Introduction

This document (Part 1), along with the *Certification Practice Statement for Buypass ACME Certificates* (Part 2) constitutes the Terms of Service for Buypass ACME Certificates.

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

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

The Subscriber may enter into more than one Terms of Service with Buypass for ACME Certificates.

2 Definitions

Term	Description
ACME client	An ACME compliant client supporting the client side operations of the ACME protocol.
Automated Certificate Management Environment (ACME)	A communication protocol for automating interactions between Certificate Authorities and their users' web servers, allowing the automated deployment of Public Key infrastructure.
Buypass Web	Websites operated by Buypass, i.e. www.buypass.no and www.buypass.com.
Certificate Policy (CP)	Named set of rules that indicates the applicability of an ACME 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 2 of the Terms of Service).
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.
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.
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.

Term	Description
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.
Revocation	Revocation of an ACME Certificate during its lifetime, i.e. when the ACME Certificate is no longer valid for some reason and must no longer be used.
ACME Certificate or Buypass ACME 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. In this document the term is used synonymously with Buypass ACME Certificate.
Subscriber	A natural person or legal entity to whom an ACME Certificate is issued and who is legally bound by the Terms of Service.
Subject Sponsor	A natural person appointed by the Subscriber to undertake the Subject's obligations under the Certificate Policy for Buypass ACME Certificates.

3 Agreement process

Subscribers must apply for ACME Certificates using an ACME client.

Prior to, or at the time of submitting a Certificate Application for Buypass ACME Certificates, the Subscriber registers/confirms the following mandatory information using the ACME protocol:
- ACME Account Public Key according to ACME protocol specifications
- Contact information for the Subject Sponsor, i.e e-mail and phone number

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

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 his SSL certificate.

4 The Subscriber's responsibilities and rights

4.1 Introduction

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

4.2 Applying for ACME Certificates

Prior to applying the Subscriber will need to register an ACME Account Public Key according to the ACME specifications and contact information for the Subject Sponsor.

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

The Subscriber must ensure that the Subject Sponsor registers proper contact information to receive notifications at any time and act upon them immediately.

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

4.3 Installation and use of ACME Certificates by the Subscriber

The Subscriber shall verify that the contents in the ACME 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 ACME 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 shall consider the ACME Certificate to be accepted 14 days after the issuance date.

ACME Certificates which are issued under this Terms of Service may only be installed on servers available on the same domain name(s) as specified in the ACME Certificate. The ACME Certificate shall not be installed on equipment which is not under the control of the Subscriber.

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

4.4 Revoking ACME 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 ACME Certificate. The ACME Certificate shall be revoked in the event of loss, misuse or suspected misuse. Failure to do so shall be regarded as coarse negligence.

The ACME Certificate shall also be revoked if the information in the certificate is incorrect or inaccurate.

If the ACME 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 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 needs to be specified.

Subscribers may submit revocation requests from the ACME client using the ACME protocol. In this case the revocation request must be signed by the ACME Account Private Key. Subscribers may also submit revocation requests to Buypass' revocation service by phone or by contacting the revocation service on Buypass Web.

The Subject Sponsor must, at any time, be 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 ACME Certificate is incorrect or invalid
- it is suspected or demonstrated that the private key has been subject to misuse or has been compromised
- the ACME 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 ACME Certificates.

The loss of a private key implies that the Subscriber must apply for a new ACME 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 may collect and store personal 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 these terms. The information will be deleted as soon as the terms are no longer applicable unless continued retention is required by law.

5.1.3   Consent
By accepting these terms, the Subscriber agrees that Buypass may process Subscriber's information and personal data as described in these terms.

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 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 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 ACME Certificates issued by Buypass is set out in the CPS in force from time to time for Buypass ACME Certificates (Part 2 of the Terms of Service). Buypass shall have no additional liability under this Terms of Service.

5.3 Revoking ACME Certificates

Buypass may revoke an ACME Certificate if the Subscriber fails to comply with the terms and conditions contained in this Terms of Service or if the certificate is used for illegal activities such as phishing or fraud, or is otherwise misused.

Buypass may also revoke an ACME Certificate if Buypass is made aware that important information in the certificate is incorrect or inaccurate.

Buypass may, at any time, notify the Subject Sponsor 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 can 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 4.4):
- Buypass obtains evidence that the private key is compromised (keyCompromize #1)
- 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.

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

6 Duration of the Terms of Service

The Terms of Service shall remain valid for as long as the ACME Certificates subject to this Terms of Service are valid or until they are revoked. The Subscriber shall be responsible for applying for new ACME Certificates before his active ACME Certificates expire.

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

Buypass may amend the contents of Part 2 of the Terms of Service (CPS) by publishing an updated CPS on Buypass Web. The new CPS shall then apply whenever the ACME Certificates are used after publication of the new CPS.

7 Legal venue and governing law

If any disagreements arise between the parties about the interpretation or legal effects of this Terms of Service, 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 Terms of Service, as well as the relationship between the Subscriber and Buypass, is regulated by Norwegian law, without regard to its choice of law principles.

8 Force Majeure

Should any extraordinary situation arise which is beyond the control of the parties and which makes it impossible to comply with this Terms of Service and which under Norwegian law is regarded as 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.

9 Contact details for Buypass

Buypass AS
PO box 4364 Nydalen
Nydalsveien 30 A
N-0402 Oslo
See Buypass Web