Terms of Use and Restrictions on Use of Qualified Certificates of PrimeSign GmbH (trust service provider primesign)

1. Information of the signatory according to Article 24 para. 2 lit d eIDAS-Regulation[1]

As far as in the following reference is made to documents, or these are partly reproduced in content, the respective document is not replaced and remains fully valid.

The documents **"Certificate Policy (CP)"** and **"Certification Practice Statement (CPS)"** extensively explain the security and certification concept in connection with qualified certificates of primesign.

1.1. The Certificate Policy (CP)

The CP describes the content of the certificate and the requirements for its secure use. It also describes the rights and obligations of the signatory and the trust service provider (TSP). The CP is the basis for the trustworthiness of a certificate. You can find a full version of the CP at http://tc.prime-sign.com/cps.

1.2. The Certification Practice Statement (CPS)

The CPS describes the technical and organizational conditions for the issuance of qualified certificates by primesign, registration and activation details for the signatory, and the liability of primesign. You can find a full version of the valid CPS at http://tc.prime-sign.com/cps.

The services of the trust service provider are under the supervision of the authorities and are subject to regular audits and in case of need.

2. Qualified Signature and Seal Certificates

The TSP primesign issues qualified certificates for natural persons and legal entities. With regard to the type of use and the validity period of a certificate, a distinction is made between a one-time certificate (with a one-time signature) and a persistent certificate. For natural persons, primesign issues persistent signing certificates and one-time certificates. For legal entities, primesign only issues persistent seal certificates.

2.1. Persistent Certificates

Persistent certificates are qualified certificates that are issued with a maximum validity period of 5 years. They can be used to repeatedly create qualified signatures or advanced/qualified seals within this validity period.

For persistent signing certificates, a natural person can be identified as follows:

- By physical presence with a registration officer
- Through an approved remote identification procedure (e.g. video identification procedure)
- Based upon a national electronic identity "eID" (e.g. ID Austria, Austrian mobile phone signature)

In all cases, a user account is set up with two-factor authentication (e.g. password and SMS-TAN). A qualified signature can be triggered based on his two-factor authentication. It is possible to sign a single document or a batch of documents. Multiple signatures to be applied to a batch of documents only need to be triggered once (a separate signature is applied to each document in the batch). Before the signing process is triggered, the single document or the documents in the batch can be viewed by the user.

For persistent seal certificates, the legal entity is identified by a registration officer. The natural person authorized to represent the entity can be identified in the same way as natural persons for the issuance of signing certificates. Depending on the product features, an advanced/qualified seal is applied upon authentication by means of one factor (e.g. password) or two factors (e.g.

[1] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

password and SMS-TAN). Here, too, a single document or a batch of documents can be sealed. Multiple seals to be applied to a batch of documents only need to be triggered once.

2.2. One-Time Certificates

Unlike persistent certificates, qualified one-time certificates are only valid for a few minutes and can only be used within a continuous transaction for creating a one-time signature. No password or the creation of a user account is required.

For one-time certificates, a natural person can be identified as follows:

- By physical presence with a registration officer
- Through an approved remote identification procedure (e.g. video identification procedure)
- Based upon a national electronic identity "eID" (e.g. ID Austria, Austrian mobile phone signature)

A one-time signature is created immediately after identification. One-time signatures can be triggered as follows:

- By a re-authentication via SMS-TAN
- Directly, if a sufficiently strong authentication (at least two-factor authentication) was performed in the course of the identification process and the identification and signature creation take place during a single signature transaction

One-time signatures can also be used to sign a single document or a batch of documents. Multiple signatures to be applied to a batch of documents only need to be triggered once. Before the signing process is triggered, the single document or the documents in the batch can be viewed by the user.

3. Legal Effect of Qualified Signatures created using Qualified primesign Certificates according § 4 SVG[2]

(1) A qualified electronic signature fulfills the legal requirement of written form within the meaning of § 886 ABGB. Other statutory or contractual formal requirements, in particular those that stipulate the involvement of a notary and/or a lawyer, remain unaffected.

(2) Testamentary dispositions cannot be effectively established in electronic form. The following declarations of intent may be drafted in electronic form only if the document contains the declaration of a notary or a lawyer that they have informed the signatory of the legal consequences of their signature:

1. Declarations of intent of family and inheritance law, which are bound to the written form or a stricter form requirement;

2. a certificate of bond (§ 1346 Abs. 2 ABGB), issued by persons outside of their commercial, business, or professional activity.

(3) An entrepreneur may not invoke a consumer's exclusion of the effectiveness of a qualified electronically signed document unless it has been individually negotiated.

4. Liability of primesign for Qualified Certificates

primesign shall be liable for its provision of services in registration, issuance of the certificate, the directory service, the revocation service, and for any of the technical components and procedures used by primesign or recommended by primesign to the signatory.

5. Technical Components and Procedures

To create qualified signatures, advanced/qualified seals and signature verification, primesign may refer to or provide specific products and procedures and recommend their use.

primesign provides a directory service for verifying certificates with the current revocation-list.

[2] Federal Law on Electronic Signatures and Trust Services for Electronic Transactions (Signatur- und Vertrauensdienstegesetz – SVG).

The use of these services is free of charge and maintains the anonymity of the user. In connection with the creation and verification of electronic signatures/seals, primesign is only liable for the use of those signature and seal products, technical components and procedures recommended by primesign to the extent primesign has specified within the recommendation.

6. Obligations of the Signatory

In order to avoid misuse and to maintain trust in qualified electronic signatures and advanced/qualified seals, the following obligations arise for the signatory:

- Obligation to register the certificate in accordance with the registration options offered by primesign
- Obligation to carefully store the signature creation data / seal creation data
- Never disclose the signature creation data / seal creation data to third parties (passing an electronic seal creation data to authorized persons is permitted)
- In addition, it must be ensured that the respective components used in the process of triggering the signature or the seal, such as PC, mobile device, OTP device, web browser, etc., are suitably protected.
  - In any case, this includes installing the latest security updates and controlling the installed applications, as well as the access to these devices.
  - Also, preventing unauthorized use of components requires the following measures depending on the device used: Completely close the web browser or lock the device (screen lock).
- Obligation to observe safety-relevant recommendations of the manufacturers of the components used.

For a signatory with a persistent certificate, the following additional obligations apply:

- Prevention of third party access to the respective signature creation data / seal creation data
  - this requires, among other things, the use of strong PINs or passwords to protect the respective signature creation data / seal creation data. A trivial PIN or a trivial password would be, for example, '123456' or a date of birth from the natural person's living environment. A strong password is characterized by the appropriate combination of the following features:
    - Length of the password
    - Use of non-guessable words, parts of words, or numbers
    - Use of special characters
    - Case sensitivity
    - Avoidance of keyboard patterns and repetitions.

    Our qualified signature creation system ensures the strength of a password by rating the individual factors and rejects passwords found to be too weak.[3] For example, while a password does not need to contain special characters to be accepted, a correspondingly longer password is required in return to ensure comparable security. We recommend relying on a balanced mix of the aforementioned criteria. In any case, the password is to be kept secret.
  - Revocation or suspension obligation using the revocation service (reasons see below)

7. Revocation of Certificates (for persistent certificates only)

7.1. Revocation Service

Through the revocation service, primesign ensures that certificates can be quickly and easily suspended or revoked at any time. This prevents misuse of the certificate. The revocation of a certificate is final. In the event of suspension, this suspension may be lifted within 10 days after appropriate authentication. If the suspension is not lifted within this period, it automatically becomes a revocation.

[3] A strong password is primarily long, without patterns ('qwertz', 'asdf'), and without repetitions ('123123'). The choice of digits and special characters is not necessarily conducive, as the example 'P @ $$ w0rd' shows. Although this meets the vast majority of password rules, it is still one of the most trivial passwords. It is better to choose 5 to 6 randomly chosen words, as these are easier to remember.

Certificates whose validity has expired can no longer be suspended or revoked. For one-time certificates whose validity is limited to a few minutes, a suspension or revocation within this period is practically not feasible.

The certificate numbers of revoked or suspended (blocked) certificates are entered by primesign in the revocation database. This revocation information is signed by primesign and is constantly updated so that the status of a certificate can be checked at any time.

Further information on revocation and suspension can be found at https://www.prime-sign.com/trustcenter and at https://tc.prime-sign.com (here you will also find the current revocation lists and all guidelines and specifications of our trust service).

At https://www.prime-sign.com/trustcenter you will also find the revocation processes and the respective access points, contact addresses, and telephone numbers under the heading "Revocation". The possibilities of revocation vary depending on the product and contract. Depending on how your qualified certificate was requested, a revocation can be obtained by, for example, revealing a revocation password (this was usually defined during registration) and / or using a personal revocation code (for example, the VOUCHER CODE for registrations via our primesign OnBoarding Service, etc.). A revocation may also require renewed legitimacy. For security reasons, a request for revocation is granted in discretion.

7.2. Mandatory Reasons for a Revocation

- The signature creation data / seal creation data has been lost.
- There are indications that they have been compromised.
- The circumstances certified in the qualified certificate have changed.

A revocation can also be obtained by the trust service provider for these reasons. If a certificate is assigned to an organization, a revocation can be made by the organization. An assignment to the organization is given if the issuance of the certificate is related to the organization and the costs for issuance, provision, and use of the certificate are borne by the organization.

8. primesign recommends

- The use of suitable signature products and procedures, which are designated as such by their manufacturer or, if applicable, by primesign.
- The use of up-to-date security software (virus protection, firewall).
- Not to use and disable trivial tools for storing and automatically entering user names or PIN / passwords, as, for example, offered by popular browsers, in the context of digital signing.

9. Contact Information

PrimeSign GmbH
Wielandgasse 2
8010 Graz

FN 405391p/ Landesgericht für ZRS Graz

Phone: +43 (316) 258300
Mail: office@prime-sign.com
Web: https://www.prime-sign.com, https://www.prime-sign.com/trustcenter, https://tc.prime-sign.com

Appendix A: Information obligations acc. Art. 13 GDPR for the processing of personal data as a trust service provider

Controller:	PrimeSign GmbH, Wielandgasse 2, 8010 Graz E-Mail: office@prime-sign.com; Phone: +43 316 25 830
Purposes of Processing:	Proof of identification of natural persons for the purpose of issuing a (qualified) certificate. There is no further use of the data for other purposes.
Legal basis:	Art 6 para 1 lit b GDPR (Fulfilment of a contract), Art 24 eIDAS-Regulation
Storage period:	30 years after expiry of the validity of the issued certificate or 30 years after issuance of the certificate (§ 10 Abs 3 SVG).
Categories of personal data:	Identity data, data to prove identity, certificate data, billing data

You are entitled to the following rights under the GDPR if the legal prerequisites are met: Right to information, correction, deletion, limitation of processing, data portability, objection to processing.

You have the right to complain to the supervisory authority if you believe that the processing of your personal data is not lawful.

Austrian Data Protection Authority, Barichgasse 40-42, 1030 Vienna, E-Mail: dsb@dsb.gv.at