primesign

digital signing, simple as that.

Contractual Requirements of PrimeSign GmbH

TSP PrimeSign

Author:
PrimeSign GmbH

Document Version: 2.0.0
Date of Issue: 22.05.2024

PUBLIC

PrimeSign GmbH
Wielandgasse 2 . 8010 Graz . Austria
T +43 (316) 25 830-0 . **E** office@prime-sign.com

cryptas.com . prime-sign.com . cryptoshop.com

Wien | Graz | Düsseldorf | Stockholm

Contractual Requirements of PrimeSign GmbH

The contractual requirements of PrimeSign GmbH consist of the following documents:

1. **Terms of Use and Restrictions on Use of Qualified Certificates** of PrimeSign GmbH
2. **General Signature Contract (natural person)** – Application for the issuance of a qualified certificate (primesign MOBILE)
3. **General Terms and Conditions** (T&C) of PrimeSign GmbH for **Qualified Electronic Certificates**

These documents are attached below in the order indicated.

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

primesign

digital signing, simple as that.

Application for the Issuance of a Qualified Certificate (primesign MOBILE)
General Signature Contract (Natural Person)

This document represents the general signature contract, concluded between the applicant (applying for the issuance of an electronic certificate; hereinafter referred to as the signatory) and PrimeSign GmbH (hereinafter referred to as primesign) during the issuing process of an electronic certificate for primesign MOBILE. Usually, the issuance takes place via electronic application processes. In this case, the personal data of the signatory and the certificate details are to be taken from the issued qualified electronic certificate and must not be given in this document.

Data of the signatory – this information is not required if the contract is concluded via electronic application systems (if a non-electronic application system is used, all fields are mandatory).			
First name:	*<First name>*	Type of ID document:	*<Type of ID-document->*
Surname:	*<Surname>*	Number of ID document:	*<Number of ID-document>*
Date of birth:	*<Date of birth>*	Issuing authority/Place:	*<Issuing authority/Place>*
E-mail address:	*<Email address>*	Date of issue:	*<Date of Issue>*
		Expiration date:	*<Expiration date>*

The signatory requests the issuance of a qualified certificate for the creation of qualified electronic signatures from primesign.

This contract is concluded by the application of the signatory on the one hand and by the acceptance of this application by primesign –(by issuing the certificate). The contract starts with the date and time of the certificate issuance and is limited in time by the date of validity of the issued certificate.

Contract Number: serial number of certificate (see certificate)
Signatory: „common name" (see certificate)
Valid until: see certificate.

For persistent certificates, the applicable options for revocation of certificates are published at the following address: https://www.prime-sign.com/trustcenter. These are not relevant, provided that the issued certificate is a one-time certificate with a validity period of a few minutes.

The **General Terms and Conditions** (GTC) for qualified certificates of PrimeSign GmbH and the **briefing of the signatory** pursuant to Article 24 para 2 lit d eIDAS-Regulation, including the additional documents cited therein, in the versions valid at the time of issuance of the certificate form an integral part of this contract. The General Terms and Conditions and the briefing of the signatory are available at https://tc.prime-sign.com.

The signatory confirms that they have read the content of the briefing as well as the terms and conditions and that they assume the duties and/or the rules of conduct contained therein.

SIGNATURES ARE NOT REQUIRED IF APPLICATION AND CONTRACT CONCLUSION ARE EFFECTED VIA ELECTRONIC APPLICATION SYSTEMS.

_____ Signatory

_____ Registration Officer

General Terms and Conditions (T&C) of PrimeSign GmbH for Qualified Electronic Certificates (version 1.1.1)

1. Subject

These terms and conditions regulate

- the conditions in conjunction with the issuance of qualified electronic certificates,
- the provision of miscellaneous services by primesign (public certificate register, revocation service),
- the signatories duties in conjunction with the secure handling of certificates.

2. Issuance of Certificates

2.1. Signature-Contract

When the certificate is issued to the signatory, the signatory concludes the signature-contract with the trust service provider „PrimeSign GmbH" (primesign).

In conjunction with the conclusion of the signature-contract the following documents (in the current version at the time of conclusion of the contract) are integral part of the contract:

- the representational T&C for qualified certificates (http://tc.prime-sign.com/agb),
- the Certificate Policy (CP, http://tc.prime-sign.com/cps),
- the Certificate Practice Statement (CPS, http://tc.prime-sign.com/cps),
- quotations provided by primesign.

These documents are provided electronically online, ready for delivery on demand by primesign under the given address.

2.2. Legal Basis

The legal basis for the application, process of issuing and usage of qualified electronic certificates are the eIDAS Regulation[1], the Austrian Signature and Trust Services Act[2] as well as the Austrian Signature and Trust Services Regulation[3] in the current version.

2.3. Proof of Identity

primesign verifies the identity of the signatories by means of an official photo ID or by another proof of equivalent reliability, that is or will be documented. Representatives of legal entities must also provide evidence of the existence of the power of authority.

2.4. Registration Authorities

primesign may conduct the identity verification and issuance of certificates either by itself or by using primesign authorized Registration Authorities (RAs). These are authorized to act on behalf of primesign in connection with the issuance of qualified certificates.

3. Costs and Payment

The issuance, provision and use of certificates are usually chargeable. The provision of the directory service and the revocation and suspension service is free of charge.

The respective prices are to be taken from specific offers from primesign. The costs for issuing, providing and using the certificate are borne by the signatory (signatory is invoice recipient) or an organization (organization is invoice recipient and bears the costs for issuing, providing and using the certificates).

Due date of costs are given in the offer.

[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.

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

[3] Austrian Regulation on electronic signatures and trust services for electronic transactions (Signatur- und Vertrauensdiensteverordnung – SVV)

3.1. Default of payment

Any delay in payment by the invoice recipient entitles primesign to deactivate the use of the certificate until payment of any fees due. In such cases, primesign shall inform the invoice recipient of the deactivation and set a reasonable grace period for the payment of due fees. If this grace period expires without payment, primesign is entitled to revoke the certificate for good cause.

3.2. Consideration of Paid Fees

In the event of termination of the signature-contract by the signatory for any unreasonable cause and in the event of cancellation or revocation by primesign for cause, there is no right for reimbursement of any fees paid.

4. Contract Duration and Termination

4.1. Contract Start, Duration, and End

The signature contract starts with the issuance of the requested certificate. The term of the contract is limited to the validity period of the issued certificate. After the expiry of the validity of the certificate, the contract ends.

4.2. Termination by the Signatory

The signatory may withdraw from the signature-contract. Withdrawal by revocation can be done in person at any authorized primesign Registration Authority or by contacting the primesign revocation service by disclosing the revocation password (chosen by the signatory during certificate application). Revocation by third parties is possible in accordance with Section 6.2. A certificate shall remain valid until the day of termination unless a revocation or a suspension of the certificate takes place earlier.

4.3. Termination by primesign

primesign shall be entitled to terminate the signature contract immediately without notice in the event of a breach of a significant obligation of the signatory arising from the agreement. The same applies mutatis mutandis to the signatory in case of breach of a material obligation arising from this agreement by primesign. As such reasons, in particular, those mentioned in the section "Revocation by primesign " of these terms and conditions come into consideration.

5. Privacy

5.1. Processing of personal Data

primesign is authorized to process all data necessary to identify the signatory and to bill for the services provided. The signatory is obliged to provide all requested documents (depending on the identification process, this can be an official photo ID, a national electronic identity "eID", etc.) and evidence upon request. In this context, documents and data are digitally recorded and stored, so that if necessary, the verified verification of the identity of the signatory can be retraced.

5.2. Duration of data storage

All data received and generated in connection with the provision of the qualified trust services shall be stored for a period of 30 years from the end of the validity period of the certificate or, failing that, 30 years from the date of the occurrence of the relevant information.

6. Revocation of Certificates

6.1. Revocation by primesign

primesign is obliged to revoke certificates issued

a) at the request of the signatory or a person authorised to represent the company or an authorised person who can prove the circumstance for a revocation and the authorization for a revocation;
b) if a suspension has not been lifted within the specified time limit;
c) if changes to the data certified in the certificate occur or the certificate contains incorrect data and primesign becomes aware of this;
d) if primesign discontinues its activities and its directory and revocation services are not taken over by another trust service provider or the Austrian Union does not ensure continuation (Section 9 (3) SVG);

e) if the supervisory authority orders a revocation or causes the suspension of the certificate primesign uses for the issuing of certificates;
f) if there is a reasonable suspicion that the certificate could be misused;
g) if the signature contract or commercial agreement has been terminated;
h) if the algorithm used as the basis of the signature has been broken.

6.2. Right of revocation by third parties

If a certificate is assigned to an organization, a revocation can be made by a third person nominated 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.

7. Revocation Obligation of the Signatory

If changes to the data certified in the certificate occur, the signatory is obliged to request the revocation of the certificates without any delay. A change of the Email address, optionally entered into the certificate, causes no revocation obligation.

8. Liability of primesign

8.1. Liability according to Article 13 eIDAS-Regulation

primesign shall be liable to any natural or legal person for intentional or negligent damages resulting from a breach of the obligations set forth in this regulation.

In the case of primesign as a qualified trust service provider, intent or negligence are assumed, unless primesign proves that damage has occurred without primesign acting intentionally or negligently.

8.2. Limitation of Liability according to Article 13 Para 2 eIDAS-Regulation

If primesign sufficiently informs its customers in advance of any restrictions on the use of the services they provide, and if these restrictions apply to third parties, primesign shall not be liable for any damage resulting from the use of the services beyond these limitations.

8.3. Liability for consequential Damages

primesign cannot be held liable for any damage caused to the signatory or to third parties due to the inability to create a digital signature at any given time.

9. Final Provisions

9.1. Specific Regulations

Terms and conditions of the signatory are not applicable.

9.2. Changes to these Terms and Conditions

Amendments to these terms and conditions which subsequently interfere with the contractual rights and obligations of the contracting parties shall be proposed to the signatory with the simultaneous possibility of objection. If the signatory does not object within 6 weeks, changes are considered to be accepted. primesign will inform the signatory of the right to object.

9.3. Formal Requirements

Changes and additions as well as all contractually relevant declarations and agreements to the signature contract as well as the changes to this clause must be made in writing.

9.4. Reception of Statements

Statements made by primesign sent to the last contact information (Email address, mobile phone number) given by the signatory shall be deemed to have been delivered to the signatory.

9.5. Applicable Law

The contractual relationship between the signatory and primesign is subject exclusively to Austrian law. Place of fulfilment is Graz. Rules that refer to foreign law are not applicable. The applicability of the UN Sales Convention is expressly excluded.

9.6. Jurisdiction

The place of jurisdiction for disputes with entrepreneurs is agreed to be the competent court at the headquarters of primesign. The local jurisdiction for disputes with consumers results from § 14 Austrian consumer protection law.