



digital signing, simple as that.

# Vertragliche Anforderungen der PrimeSign GmbH

**VDA PrimeSign**

Autor:  
PrimeSign GmbH

Dokumenten-Version: 1.0.0  
Ausgabedatum: 13.02.2023

**PUBLIC**

**PrimeSign GmbH**

Wielandgasse 2 . 8010 Graz . Austria

T +43 (316) 25 830-0 . E [office@prime-sign.com](mailto:office@prime-sign.com)

[cryptas.com](https://cryptas.com) . [prime-sign.com](https://prime-sign.com) . [cryptoshop.com](https://cryptoshop.com)

Wien | Graz | Düsseldorf | Stockholm

## **Vertragliche Anforderungen der PrimeSign GmbH**

Die vertraglichen Anforderungen der PrimeSign GmbH setzen sich aus folgenden Dokumenten zusammen:

1. **Bedingungen zur Nutzung und Nutzungsbeschränkungen für qualifizierte Zertifikate** der PrimeSign GmbH
2. **Allgemeiner Signaturvertrag (natürliche Person)** - Antrag auf Ausstellung eines qualifizierten Zertifikats (primesign MOBILE)
3. **Allgemeine Geschäftsbedingungen (AGB)** der PrimeSign GmbH für **qualifizierte Zertifikate**

Diese Dokumente sind nachstehend in der entsprechenden Reihenfolge beigelegt.

## **Bedingungen zur Nutzung und Nutzungsbeschränkungen für qualifizierte Zertifikate der PrimeSign GmbH (Vertrauensdiensteanbieter primesign)**

### **1. Unterrichtung gemäß Artikel 24 Abs 2 lit d eIDAS-VO<sup>1</sup>**

Soweit in der Folge auf Dokumente verwiesen wird bzw. diese zum Teil inhaltlich wiedergegeben werden, so wird dadurch das jeweilige Dokument nicht ersetzt, sondern dieses bleibt vollinhaltlich gültig.

In den Dokumenten „**Anwendungsvorgabe** (Certificate Policy, CP)“ und „**Zertifizierungsrichtlinie** (Certification Practice Statement, CPS)“ wird das Sicherheits- und Zertifizierungskonzept im Zusammenhang mit qualifizierten Zertifikaten der primesign umfassend erläutert.

#### **1.1. Die Anwendungsvorgabe (Certificate Policy, CP)**

In der Anwendungsvorgabe werden der Inhalt des Zertifikats und die Voraussetzungen zu dessen sicheren Verwendung dargestellt. Zudem werden hier auch die Rechte und Pflichten des/der Unterzeichners/in und des Vertrauensdiensteanbieters (VDA) beschrieben. Die Anwendungsvorgabe ist Grundlage der Vertrauenswürdigkeit eines Zertifikats. Sie finden eine vollständige Version der Anwendungsvorgabe unter <http://tc.prime-sign.com/cps>.

#### **1.2. Die Zertifizierungsrichtlinie (Certification Practice Statement, CPS)**

In der Zertifizierungsrichtlinie werden die technischen und organisatorischen Bedingungen zur Ausstellung eines qualifizierten Zertifikats durch primesign und Details zu Registrierung und Aktivierung für den/die Unterzeichner/in sowie zur Haftung der primesign beschrieben. Sie finden eine vollständige Version der gültigen Zertifizierungsrichtlinie unter <http://tc.prime-sign.com/cps>.

Die Dienste des Vertrauensdiensteanbieters stehen unter behördlicher Aufsicht und werden regelmäßig und im Anlassfall einer Prüfung unterzogen.

### **2. Qualifizierte Signatur- und Siegelzertifikate**

Der VDA primesign stellt qualifizierte Zertifikate für natürliche und juristische Personen aus. Hinsichtlich der Art der Nutzung und der Gültigkeitsdauer des Zertifikats wird zwischen Einmalzertifikaten (mit Einmalsignatur) und persistenten Zertifikaten unterschieden. Für natürliche Personen werden persistente Signaturzertifikate, also auch Einmalzertifikate ausgestellt. Für juristische Personen werden ausschließlich persistente Siegelzertifikate ausgestellt.

#### **2.1. Persistente Zertifikate**

Persistente Zertifikate sind qualifizierte Zertifikate, die mit einer maximalen Gültigkeitsdauer von 5 Jahren ausgestellt werden und innerhalb dieses Gültigkeitszeitraums zur wiederholten Erstellung von qualifizierten Signaturen bzw. fortgeschrittenen/qualifizierten Siegeln genutzt werden können.

Für persistente Signaturzertifikate kann die Identifikation der natürlichen Person auf folgenden Wegen erfolgen:

- In persönlicher Anwesenheit bei einem Registration Officer
- Mittels eines zugelassenen Distanz-Identifikationsverfahrens (z.B. Video-Identifikationsverfahren)
- Auf Basis einer nationalen elektronischen Identität „eID“ (z.B. ID Austria, österreichische Handy-Signatur)

In allen Fällen erfolgt die Einrichtung eines User-Accounts mit Zwei-Faktor-Authentifizierung (z.B. Passwort und SMS-TAN). Eine qualifizierte Signatur kann auf Basis dieser Zwei-Faktor-Authentifizierung ausgelöst werden. Es ist möglich, mit einer Signaturauslösung ein Einzeldokument oder auch ein Stapel von Dokumenten zu signieren (auf jedes Dokument im Stapel wird eine separate Signatur aufgebracht). Vor der Signaturauslösung kann das Einzeldokument oder die Dokumente im Stapel nochmals angesehen werden.

---

<sup>1</sup> VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

Für persistente Siegelzertifikate erfolgt die Identifikation der juristischen Person mittels eines Registration Officers. Die Identifikation der vertretungsbefugten natürlichen Person kann auf den gleichen Wegen wie für natürliche Personen zur Ausstellung von Signaturzertifikaten erfolgen. Ein fortgeschrittenes/qualifiziertes Siegel wird, in Abhängigkeit von der Produktausprägung, anhand einer Authentifizierung mittels eines Faktors (z.B. Passwort) oder zwei Faktoren (z.B. Passwort und SMS-TAN) aufgebracht. Auch hier ist es möglich mit einer Auslösung ein Einzeldokument oder einen Stapel von Dokumenten zu siegeln.

## **2.2. Einmalzertifikate**

Im Gegensatz zu persistenten Zertifikaten sind qualifizierte Einmalzertifikate nur wenige Minuten gültig und können nur innerhalb einer durchgängigen Transaktion für die einmalige Signaturerstellung (Einmalsignatur) verwendet werden. Die Einrichtung eines User-Accounts und somit auch die Festlegung eines Passworts für diesen Account entfällt.

Für Einmalzertifikate kann die Identifikation der natürlichen Person auf folgenden Wegen erfolgen:

- In persönlicher Anwesenheit bei einem Registration Officer
- Mittels eines zugelassenen Distanz-Identifikationsverfahrens (z.B. Video-Identifikationsverfahren)
- Auf Basis einer nationalen elektronischen Identität „eID“ (z.B. ID Austria, österreichische Handy-Signatur)

Die Einmalsignatur wird direkt nach der Identifikation ausgelöst. Folgende Varianten sind möglich:

- Auslösung durch eine erneute Authentifizierung mittels SMS-TAN
- Direkte Auslösung, wenn eine ausreichend starke Authentifizierung (zumindest Zwei-Faktor-Authentifizierung) im Zuge des Identifikationsvorgangs vorliegt sowie Identifikation und Signatur in einer Transaktion erfolgen

Auch bei der Einmalsignatur können mit einer Signaturauslösung ein Einzeldokument oder auch ein Stapel von Dokumenten signiert werden. Vor der Signaturauslösung kann das Einzeldokument oder die Dokumente im Stapel nochmals angesehen werden.

## **3. Rechtswirkung von mit qualifizierten Zertifikaten der primesign erstellten qualifizierten Signaturen gemäß § 4 SVG<sup>2</sup>**

(1) Eine qualifizierte elektronische Signatur erfüllt das rechtliche Erfordernis der Schriftlichkeit im Sinne des § 886 ABGB. Andere gesetzliche oder vertragliche Formerfordernisse, insbesondere solche, die die Beziehung eines/einer Notars/in oder eines/einer Rechtsanwaltes/in vorsehen, bleiben unberührt.

(2) Letztwillige Verfügungen können in elektronischer Form nicht wirksam errichtet werden. Folgende Willenserklärungen können nur dann in elektronischer Form wirksam abgefasst werden, wenn das Dokument die Erklärung eines/einer Notars/in oder eines/einer Rechtsanwalts/in enthält, dass er den/die Unterzeichner/in über die Rechtsfolgen seiner Signatur aufgeklärt hat:

1. Willenserklärungen des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind;
2. eine Bürgschaftserklärung (§ 1346 Abs. 2 ABGB), die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird.

(3) Ein/e Unternehmer/in kann sich gegenüber einem/einer Verbraucher/in nicht auf den Ausschluss der Wirksamkeit eines qualifiziert elektronisch signierten Dokuments berufen, es sei denn dieser wurde einzeln ausgehandelt.

## **4. Haftung der primesign für qualifizierte Zertifikate**

primesign haftet für ihre Leistungserbringung in der Registrierung, der Ausstellung des Zertifikats, des Verzeichnisdienstes, des Widerrufsdienstes und für die von ihr eingesetzten bzw. dem/der Unterzeichner/in allfällig von ihr empfohlenen technischen Komponenten und Verfahren.

---

<sup>2</sup> Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG).

## 5. Technische Komponenten und Verfahren

Zur Erstellung qualifizierter Signaturen und fortgeschrittener/qualifizierter Siegel sowie zur Signaturprüfung kann primesign auf spezielle Produkte und Verfahren verweisen oder diese zur Verfügung stellen und deren Verwendung empfehlen.

primesign stellt zur Prüfung von Zertifikaten einen Verzeichnisdienst mit der jeweils aktuellen Widerrufs- und Sperreliste bereit.

Die Verwendung dieser Dienste ist unentgeltlich und erfolgt unter Wahrung der Anonymität des/der Nutzers/in. Im Zusammenhang mit der Erstellung und Prüfung von elektronischen Signaturen/Siegeln haftet primesign bei der Verwendung der allfällig von ihr empfohlenen Signatur- und Siegelprodukte, technischen Komponenten und Verfahren ausschließlich in dem von ihr mit der Empfehlung ausgewiesenen Umfang.

## 6. Pflichten des/der Unterzeichners/in

Zur Vermeidung von Missbrauch und zur Wahrung des Vertrauens in qualifizierte elektronische Signaturen bzw. fortgeschrittene/qualifizierte Siegel ergeben sich für Unterzeichner/innen folgende Pflichten:

- Pflicht zur Registrierung des Zertifikats gemäß den angebotenen Registrierungsmöglichkeiten des VDA
- Pflicht zur sorgfältigen Verwahrung der Signaturerstellungsdaten/Siegelerstellungsdaten
- Unterlassung der Weitergabe der Signaturerstellungsdaten/Siegelerstellungsdaten an Dritte (Die Weitergabe von elektronischen Siegelstellungsdaten an autorisierte Personen ist zulässig)
- Zusätzlich ist sicherzustellen, dass die jeweiligen - im Zuge der Auslösung der Signatur bzw. des Siegels - verwendeten Komponenten, wie PC, Mobilfunkgerät, OTP-Device, Webbrowser etc. geeignet abgesichert sind.
  - o Dazu zählt jedenfalls das Einspielen der jeweils aktuellen Sicherheitsupdates und eine Kontrolle über die installierten Anwendungen sowie über den Zugriff auf diese Geräte.
  - o Zum Schutz vor unbefugter Nutzung der Komponenten sind zudem je nach eingesetztem Gerät, folgende Maßnahmen erforderlich: Vollständiges Schließen des Webbrowsers oder Sperre des Geräts (Bildschirm Sperre).
- Pflicht zur Beachtung sicherheitsrelevanter Empfehlungen der Hersteller der verwendeten Komponenten

Für Unterzeichner/innen mit persistentem Zertifikat gelten zusätzlich folgende weitere Pflichten:

- Verhinderung von Zugriffen durch Dritte auf die jeweiligen Signaturerstellungsdaten/Siegelerstellungsdaten
    - o Dies bedingt u.a. die Wahl starker PINs bzw. Passwörter zum Schutz der jeweiligen Signaturerstellungsdaten/Siegelerstellungsdaten. Eine triviale PIN bzw. ein triviales Passwort wäre beispielsweise '123456' oder ein Geburtsdatum aus dem Lebensumfeld der natürlichen Person. Ein starkes Passwort zeichnet die geeignete Kombination folgender Merkmale aus:
      - Länge des Passworts
      - Verwendung nicht erratbarer Wörter, Wortteile oder Nummern
      - Verwendung von Sonderzeichen
      - Verwendung von Groß-/Kleinschreibung
      - Vermeidung von Tastaturmustern und Wiederholungen
- Unser qualifiziertes Signaturerstellungssystem stellt die Stärke des eingegebenen Passworts aufgrund der Gesamtbewertung der Einzelfaktoren sicher und lehnt in der Gesamtbetrachtung zu schwache Passwörter ab<sup>3</sup>. Um akzeptiert zu werden, muss ein Passwort bspw. keine Sonderzeichen enthalten, im Gegenzug ist aber ein entsprechend längeres Passwort erforderlich, um eine vergleichbare Sicherheit zu gewährleisten. Grundsätzlich empfehlen wir, auf eine ausgewogene Mischung der vorgenannten Kriterien zu setzen. In jedem Fall ist das Passwort geheim zu halten.
- Widerrufs- bzw. Aussetzungspflicht unter Inanspruchnahme des Widerrufsdienstes (Gründe siehe unten)

---

<sup>3</sup> Ein starkes Passwort ist in erster Linie lang, ohne Muster ('qwertz', 'asdf') und ohne Wiederholungen ('123123'). Die Wahl von Ziffern und Sonderzeichen ist hingegen nicht zwangsläufig förderlich, wie das Beispiel 'P@\$\$wOrd' zeigt. Damit erfüllt man zwar die allermeisten Passwortrichtlinien, es handelt sich dabei aber trotzdem um eines der trivialsten Passwörter. Besser ist die Wahl von 5 bis 6 zufällig gewählter Worte, da diese leichter zu merken sind.

## 7. Widerruf von Zertifikaten (nur für persistente Zertifikate)

### 7.1. Widerrufsdienst

Durch den Widerrufsdienst stellt primesign jederzeit sicher, dass Zertifikate schnell und einfach ausgesetzt bzw. widerrufen werden können. So kann ein Missbrauch des Zertifikats verhindert werden. Der Widerruf eines Zertifikats ist endgültig. Im Falle einer Aussetzung kann eine Aufhebung dieser Aussetzung binnen 10 Tagen nach entsprechender Authentisierung erfolgen. Andernfalls geht die Aussetzung nach Ablauf der 10 Tage automatisch in einen Widerruf über.

Zertifikate deren zeitliche Gültigkeit abgelaufen ist können nicht mehr ausgesetzt oder widerrufen werden. Bei Einmalzertifikaten, deren Gültigkeit auf wenige Minuten beschränkt ist, ist eine Aussetzung bzw. ein Widerruf innerhalb dieser Zeitspanne praktisch nicht durchführbar.

Die Zertifikatsnummern widerrufener oder ausgesetzter (gesperrter) Zertifikate werden durch primesign in der Widerrufsdatenbank eingetragen. Diese von primesign signierten Widerrufsinformationen werden laufend aktualisiert. Somit kann jederzeit der Status eines Zertifikats geprüft werden.

Weitere Informationen zu Widerruf und Aussetzung finden Sie unter <https://www.prime-sign.com/trustcenter> sowie unter <https://tc.prime-sign.com> (hier finden Sie auch die aktuellen Widerrufslisten sowie alle Richtlinien und Vorgaben unseres Vertrauensdienstes).

Unter <https://www.prime-sign.com/trustcenter> finden Sie unter der Rubrik „Widerruf“ auch die jeweils verfügbaren Widerrufprozesse und die jeweiligen Zugangspunkte, Kontaktadressen und Telefonnummern. Die Möglichkeiten des Widerrufs variieren je nach Produkt und Vertrag. Je nachdem wie Ihr qualifiziertes Zertifikat beantragt wurde, kann ein Widerruf beispielsweise unter Bekanntgabe eines Widerrufskenworts (dieses wurde in der Regel während der Registrierung festgelegt) und/oder anhand eines persönlichen Widerruf-Codes (zum Beispiel anhand des Registrierungscode bei Registrierungen über das primesign OnBoarding Service) erwirkt werden. Ein Widerruf kann auch eine erneute Legitimation erfordern. Aus Sicherheitsgründen wird im Ermessensfall einem Widerrufs Antrag stattgegeben.

### 7.2. Zwingende Gründe für einen Widerruf

- Die Signaturerstellungsdaten / Siegelerstellungsdaten sind abhandengekommen.
- Es bestehen Anhaltspunkte für deren Kompromittierung.
- Die im qualifizierten Zertifikat bescheinigten Umstände haben sich geändert.

Ein Widerruf kann aus diesen Gründen auch seitens des Vertrauensdienstes erwirkt werden. Ist ein Zertifikat einer Organisation zugeordnet, kann ein Widerruf auch durch die Organisation erfolgen (Eine Zuordnung zur Organisation ist gegeben, wenn die Ausstellung des Zertifikats in Verbindung mit der Organisation steht sowie die Kosten für Ausstellung, Bereitstellung und Nutzung des Zertifikats von der Organisation übernommen werden).

## 8. primesign empfiehlt

- Die Verwendung geeigneter Signaturprodukte und -verfahren, die von deren Hersteller oder gegebenenfalls auch von primesign als solche ausgewiesen werden.
- Den Einsatz aktueller Sicherheitssoftware (Viruschutz, Firewall).
- Triviale Werkzeuge zur Speicherung und automatischer Eingabe von User-Namen oder PIN/Passwörtern, wie sie z.B. von gängigen Browsern angeboten werden, in dem Zusammenhang nicht zu nutzen und zu deaktivieren.

## 9. Kontaktdaten

PrimeSign GmbH  
Wielandgasse 2  
8010 Graz

FN 405391p/ Landesgericht für ZRS Graz

Tel.: +43 (316) 258300  
Mail: [office@prime-sign.com](mailto:office@prime-sign.com)  
Web: <https://www.prime-sign.com>,  
<https://www.prime-sign.com/trustcenter>,  
<https://tc.prime-sign.com>

**Anhang A: Informationspflichten gem. Art 13 DSGVO für Verarbeitung persönlicher Daten im Rahmen unserer Tätigkeiten als Vertrauensdienst primesign**

Für die Verarbeitung Verantwortlicher:	PrimeSign GmbH, Wielandgasse 2, 8010 Graz E-Mail: office@prime-sign.com; Telefon: +43 316 25 830
Zweck der Verarbeitung:	Nachweis der Identifikation natürlicher Personen zum Zweck der Ausstellung eines (qualifizierten) Zertifikates. Es erfolgt keine Weiterverwendung der Daten für andere Zwecke.
Rechtsgrundlage:	Art 6 Abs 1 lit b DSGVO (Erfüllung eines Vertrages), Art 24 eIDAS-VO
Dauer der Aufbewahrung:	30 Jahre nach Ablauf der Gültigkeit des ausgestellten Zertifikats bzw. 30 Jahre ab Ausstellung des Zertifikats (§ 10 Abs 3 SVG)
Verarbeitete Daten:	Identitätsdaten, Daten zum Nachweis der Identität, Zertifikatsdaten

Ihnen stehen bei Vorliegen der gesetzlichen Voraussetzungen folgende Rechte gemäß DSGVO zu: Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch gegen die Verarbeitung.

Sie haben das Recht, sich bei der folgenden Aufsichtsbehörde zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt: Österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Wien, E-Mail: dsb@dsb.gv.at

digital signing, simple as that.

**Antrag auf Ausstellung eines qualifizierten Zertifikats (primesign MOBILE)****Allgemeiner Signaturvertrag (natürliche Person)**

Should you require an English translation of the contract, please contact us directly. The given German version is legally binding.

Dieses Dokument ist der allgemeine Signaturvertrag, der zwischen dem/der Antragsteller/Antragstellerin (beantragt die Ausstellung eines Zertifikats; in Folge Unterzeichner/Unterzeichnerin genannt) und der PrimeSign GmbH (in Folge primesign genannt) im Wege der Zertifikatsausstellung für primesign MOBILE geschlossen wird. In der Regel wird das Zertifikat über elektronische Antragsprozesse ausgestellt. Die persönlichen Daten des/der Unterzeichners/in sowie die Zertifikatdetails sind somit dem ausgestellten qualifizierten Zertifikat zu entnehmen und müssen in diesem Fall nicht in diesem Dokument angegeben werden.

Daten des/der Unterzeichners/in – diese Angaben entfallen bei Abschluss über elektronische Antragssysteme (bei Abschluss über nichtelektronische Antragssysteme sind alle Felder verpflichtend auszufüllen)			
Vorname:	<Vorname>	Ausweisart:	<Ausweisart>
Nachname:	<Nachname>	Ausweisnummer:	<Ausweisnummer>
Geburtsdatum:	<Geburtsdatum>	Behörde/Ort:	<Behörde/Ort>
E-Mail-Adresse:	<E-Mail-Adresse>	Ausstellungsdatum:	<Ausstellungsdatum>
		Ablaufdatum:	<Ablaufdatum>

Der/die Unterzeichner/Unterzeichnerin beantragt die Ausstellung eines qualifizierten Zertifikats zur Erstellung qualifizierter elektronischer Signaturen durch die Firma primesign.

Dieser Vertrag kommt durch den Antrag des/der Unterzeichners/in einerseits und durch die Annahme dieses Antrages der primesign - durch Ausstellen des Zertifikats - zustande. Als Vertragsbeginn gilt der Zeitpunkt der Zertifikatsausstellung. Die Vertragsdauer ist befristet mit der Gültigkeitsdauer des ausgestellten Zertifikats.

Vertragsnummer: Seriennummer des Zertifikats, siehe Zertifikat  
Zertifikatsinhaber/in: Siehe „Common Name“ im Zertifikat  
Gültigkeitsdauer: Siehe Zertifikat

Für persistente Zertifikate sind die jeweils geltenden Widerrufsmöglichkeiten unter folgender Adresse veröffentlicht: <https://www.prime-sign.com/trustcenter>. Diese sind nicht relevant, sofern es sich bei dem ausgestellten Zertifikat um ein Einmalzertifikat mit einer zeitlichen Gültigkeit von wenigen Minuten handelt.

Die Allgemeinen Geschäftsbedingungen (AGB) der PrimeSign GmbH für qualifizierte Zertifikate und die **Unterrichtung des/der Unterzeichners/in** gemäß Artikel 24 Abs 2 lit d eIDAS-VO, inklusive der darin angeführten weiterführenden Dokumente in den zum Zeitpunkt der Ausstellung gültigen Fassungen bilden einen integrierenden Bestandteil dieses Vertrages. Die AGB und Unterrichtung des/der Unterzeichners/in sind unter <https://tc.prime-sign.com> verfügbar.

Der/die Unterzeichner/in bestätigt, den Inhalt der Unterrichtung sowie die AGB zur Kenntnis genommen zu haben und die darin angeführten Pflichten zu übernehmen bzw. die darin enthaltenen Verhaltensregeln zu befolgen.

**UNTERSCHRIFTEN ENTFALLEN BEI ANTRAG UND  
VERTRAGSABSCHLUSS ÜBER ELEKTRONISCHE ANTRAGSSYSTEME.**

---

Unterschrift des/der Unterzeichners/in

---

Unterschrift des Registration Officers

digital signing, simple as that.

## Allgemeine Geschäftsbedingungen (AGB) der PrimeSign GmbH für qualifizierte Zertifikate (Version 1.1.1)

### 1. Gegenstand der AGB

Diese AGB regeln

- die Bedingungen im Zusammenhang mit der Ausstellung qualifizierter Zertifikate,
- die Bereitstellung sonstiger Dienste und Dienstleistungen durch primesign; (öffentlicher Verzeichnisdienst, Widerrufsdienst)
- die Pflichten des/der Unterzeichners/in im Zusammenhang mit dem sicheren Umgang mit Zertifikaten.

### 2. Zertifikatsausstellung

#### 2.1. Signaturvertrag

Bei Zertifikatsausstellung schließt der/die Unterzeichner/in mit dem Vertrauensdiensteanbieter „PrimeSign GmbH“ (primesign) einen Signaturvertrag ab.

Im Zusammenhang mit dem Abschluss des Signaturvertrages werden folgende Dokumente (in der zum Zeitpunkt des Vertragsabschlusses geltenden Fassung) ebenfalls Vertragsbestandteil:

- Die gegenständlichen AGB für qualifizierte Zertifikate (<http://tc.prime-sign.com/agb>),
- die Anwendungsvorgabe (CP, <http://tc.prime-sign.com/cps>),
- die Zertifizierungsrichtlinie (CPS, <http://tc.prime-sign.com/cps>),
- Angebote der primesign.

Diese Dokumente werden von primesign im Internet unter den oben angegebenen Adressen elektronisch abrufbereit gehalten.

#### 2.2. Rechtsgrundlagen

Für die Beantragung, für das Verfahren zur Ausstellung sowie für die Verwendung eines qualifizierten Zertifikats gelten die Vorschriften der eIDAS-VO<sup>1</sup>, das SVG<sup>2</sup> und die SVV<sup>3</sup> in der jeweils aktuellen Fassung.

#### 2.3. Identitätsfeststellung

primesign überprüft die Identität der Unterzeichner bzw. Unterzeichnerinnen anhand eines amtlichen Lichtbildausweises oder durch einen anderen in seiner Zuverlässigkeit gleichwertigen, dokumentierten oder zu dokumentierenden Nachweis. Vertreter von juristischen Personen haben darüber hinaus einen Nachweis über das Bestehen der Vertretungsbefugnisse vorzulegen.

#### 2.4. Registrierungsstellen

primesign kann die Identitätsprüfung und Zertifikatsausstellung entweder selbst oder unter Beiziehung von durch primesign autorisierten Registrierungsstellen (Registration Authority, RA) durchführen. Diese sind befugt, im Namen der primesign im Zusammenhang mit der Ausstellung qualifizierter Zertifikate tätig zu werden.

### 3. Kosten und Zahlung

Die Ausstellung, Bereitstellung und Nutzung von Zertifikaten ist in der Regel kostenpflichtig. Die Bereitstellung des Verzeichnisdienstes und des Widerrufs- und Sperrdienstes erfolgt kostenlos.

Die jeweiligen Preise sind den konkreten Angebot der primesign zu entnehmen. Die Kosten trägt der/die Unterzeichner/in (Unterzeichner/in ist Rechnungsempfänger/in) oder eine Organisation (Organisation ist Rechnungsempfänger und trägt die Kosten für die Ausstellung, Bereitstellung und Nutzung der Zertifikate)

Die Kosten werden gemäß des Angebots fällig.

<sup>1</sup> VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

<sup>2</sup> Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz - SVG)

<sup>3</sup> Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung - SVV)

digital signing, simple as that.

### 3.1. Zahlungsverzug

Ein allfälliger Zahlungsverzug des/der Rechnungsempfängers/in berechtigt primesign die Nutzung des Zertifikates bis zur Zahlung fälliger Entgelte zu sperren. In diesen Fällen wird primesign den/die Rechnungsempfänger/in über die Nutzungssperre informieren und eine angemessene Nachfrist für die Zahlung fälliger Entgelte setzen. Verstreicht diese Nachfrist ohne Zahlungseingang ist primesign berechtigt, das Zertifikat aus wichtigem Grund zu widerrufen.

### 3.2. Anrechnung bezahlter Entgelte

Im Falle einer Kündigung des Signaturvertrags durch den/die Unterzeichner/in aus nicht wichtigem Grund und in Fällen einer Kündigung oder Widerruf durch primesign aus wichtigem Grund besteht kein Anspruch auf Rückerstattung entrichteter Entgelte.

## 4. Vertragsdauer und Beendigung

### 4.1. Vertragsbeginn, -dauer und -ende

Der Signaturvertrag kommt nach Antrag durch den/die Unterzeichner/in durch Ausstellung des Zertifikats zustande. Die Laufzeit des Vertrages ist auf die Gültigkeitsdauer des ausgestellten Zertifikats beschränkt. Nach Ablauf der Gültigkeit des Zertifikats endet der Vertrag.

### 4.2. Kündigung durch den/die Unterzeichner/in

Der/die Unterzeichner/in hat die Möglichkeit, vom Signaturvertrag zurückzutreten. Die Rücktrittserklärung durch Widerruf kann persönlich in einer von primesign autorisierten Registrierungsstelle oder unter Angabe des Passworts für den Widerruf (Widerrufskennwort) beim Widerrufsdienst der primesign erfolgen. Ein Widerruf durch Dritte ist gemäß Abschnitt 6.2 möglich. Die Gültigkeit der Zertifikate bleibt bis zum Rücktrittsstichtag aufrecht, wenn nicht früher ein Widerruf oder eine Aussetzung der Zertifikate erfolgt.

### 4.3. Kündigung durch primesign

primesign ist berechtigt, im Falle der Verletzung einer aus dem Signaturvertrag entstandenen wesentlichen Pflicht des/der Unterzeichners/in, den Vertrag ohne Einhaltung einer Kündigungsfrist zu lösen. Sinngemäß gilt dies auch umgekehrt für den/die Unterzeichner/in bei Verletzung einer aus dem Signaturvertrag entstandenen wesentlichen Pflicht durch primesign. Als solche Gründe kommen insbesondere jene im Abschnitt "Widerruf durch primesign" dieser AGB genannten Punkte in Betracht.

## 5. Datenschutz

### 5.1. Verarbeitung von personenbezogenen Daten

primesign ist dazu befugt, alle notwendigen Daten zur Identifikation des/der Unterzeichners/in und zur Verrechnung der erbrachten Leistungen zu verwenden. Der/die Unterzeichner/in ist dazu verpflichtet, auf Verlangen alle angeforderten Dokumente (abhängig vom Identifikationsverfahren kann das ein amtlicher Lichtbildausweis, eine nationale elektronische Identität „eID“, etc. sein) und Nachweise vorzulegen. In diesem Zusammenhang werden Dokumente und Daten digital erfasst und gespeichert, damit bei Bedarf die erfolgte Überprüfung der Identität des/der Unterzeichners/in nachvollzogen werden kann.

### 5.2. Dauer der Datenspeicherung

Alle im Zusammenhang mit der Erbringung der qualifizierten Vertrauensdienste ausgegebenen und empfangenen Daten werden für die Dauer von 30 Jahren gerechnet ab dem im Zertifikat eingetragenen Ende der Gültigkeit oder mangels eines solchen 30 Jahre ab dem Zeitpunkt des Anfallens von einschlägigen Informationen gespeichert.

## 6. Widerruf von Zertifikaten

### 6.1. Widerruf durch primesign

primesign ist zum Widerruf der von ihr ausgestellten Zertifikate verpflichtet

- a) auf Antrag des/der Unterzeichners/in oder einer vertretungsbefugten bzw. bevollmächtigten Person, die den Umstand für einen Widerruf und die Berechtigung für diesen nachweisen kann;
- b) wenn eine Aussetzung nicht innerhalb der vorgegebenen Frist aufgehoben wurde;

digital signing, simple as that.

- c) wenn Änderungen der im Zertifikat bescheinigten Daten eintreten oder das Zertifikat falsche Daten enthält und primesign davon Kenntnis erlangt;
- d) wenn primesign ihre Tätigkeit einstellt und ihre Verzeichnis- und Widerrufsdienste nicht von einem anderen Vertrauensdiensteanbieter übernommen werden bzw. der Bund nicht für eine Weiterführung Sorge trägt (§ 9 Abs 3 SVG)
- e) wenn die Aufsichtsstelle einen Widerruf anordnet oder die Aussetzung des primesign Zertifikats zur Zertifikatsausstellung veranlasst;
- f) wenn der begründete Verdacht besteht, dass das Zertifikat missbräuchlich verwendet werden könnte;
- g) wenn der Signaturvertrag oder die zugrunde liegende kommerzielle Vereinbarung gekündigt wurde;
- h) der Algorithmus als Grundlage der Signatur gebrochen wurde.

## 6.2. Widerrufsrecht durch Dritte

Ist ein Zertifikat einer Organisation zugeordnet, kann ein Widerruf durch von der Organisation nominierte Dritte erfolgen. Eine Zuordnung zur Organisation ist gegeben, wenn die Ausstellung des Zertifikats in Verbindung mit der Organisation steht sowie die Kosten für Ausstellung, Bereitstellung und Nutzung des Zertifikats von der Organisation übernommen werden.

## 7. Widerrufspflicht des/der Unterzeichners/in

Wenn Änderungen der im Zertifikat bescheinigten Daten eintreten, ist der/die Unterzeichner/in verpflichtet den Widerruf dieser Zertifikate unverzüglich zu beantragen. Eine Veränderung der optional ins Zertifikat eingetragenen E-Mail-Adresse löst keine Widerrufspflicht aus.

## 8. Haftung der primesign

### 8.1. Haftung nach Artikel 13 eIDAS-VO

primesign haftet für alle natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügten Schäden, die auf eine Verletzung der in dieser Verordnung festgelegten Pflichten zurückzuführen sind.

Bei primesign als qualifiziertem Vertrauensdiensteanbieter wird von Vorsatz oder Fahrlässigkeit ausgegangen, es sei denn, primesign weist nach, dass Schaden entstanden ist, ohne dass primesign vorsätzlich oder fahrlässig gehandelt hat.

### 8.2. Haftungseinschränkung nach Artikel 13 Abs 2 eIDAS-VO

Unterrichtet primesign ihre Kunden im Voraus hinreichend über Beschränkungen der Verwendung der von ihnen erbrachten Dienste und sind diese Beschränkungen für dritte Beteiligte ersichtlich, so haftet primesign nicht für Schäden, die bei einer über diese Beschränkungen hinausgehenden Verwendung der Dienste entstanden sind.

### 8.3. Haftung für Folgeschäden

primesign haftet nicht für Schäden, die dem/der Unterzeichner/in oder Dritten dadurch entstanden sind, dass die Erstellung einer digitalen Signatur zu einem bestimmten Zeitpunkt nicht möglich war.

## 9. Schlussbestimmungen

### 9.1. Besondere Bedingungen

Allfällige AGB des/der Unterzeichners/in finden keine Anwendung.

### 9.2. Änderungen dieser AGB

Änderungen dieser AGB, die nachträglich in die vertraglichen Rechte und Pflichten der Vertragsparteien eingreifen, werden dem/der Unterzeichner/in unter gleichzeitiger Möglichkeit des Widerspruchs vorgeschlagen. Widerspricht der/die Unterzeichner/in nicht binnen 6 Wochen, gilt die Änderung als von ihm/ihr genehmigt. Darauf wird primesign den/die Unterzeichner/in im Änderungsvorschlag hinweisen.

### 9.3. Formvorschriften

Änderungen und Ergänzungen sowie alle vertragsrelevanten Erklärungen und Absprachen zum Signaturvertrag ebenso wie die Änderungen dieser Klausel bedürfen für ihre Wirksamkeit der Schriftform.

digital signing, simple as that.

#### **9.4. Zugang von Erklärungen**

Erklärungen der primesign, die an die letzte von dem/der Unterzeichner/in bekannt gegebene Kontaktinformation (E-Mail-Adresse, Mobiltelefonnummer) versandt wurden, gelten diesem als zugestellt.

#### **9.5. Anzuwendendes Recht**

Das Vertragsverhältnis zwischen dem/der Unterzeichner/in und primesign unterliegt ausschließlich österreichischem Recht. Erfüllungsort ist Graz. Normen, die auf ausländisches Recht verweisen, kommen nicht zur Anwendung. Die Anwendbarkeit des UN-Kaufrechts wird ausdrücklich ausgeschlossen.

#### **9.6. Gerichtsstand**

Als Gerichtsstand für Streitigkeiten mit Unternehmern wird das sachlich zuständige Gericht am Sitz der primesign vereinbart. Die örtliche Zuständigkeit für Streitigkeiten mit Verbrauchern ergibt sich aus § 14 Konsumentenschutzgesetz.