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

1. Unterrichtung gemäß Artikel 24 Abs 2 lit d eIDAS-VO[1]

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.

[1] 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[2]

(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 Beiziehung 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.

[2] 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 Sperrliste 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 Siegelerstellungsdaten 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.
    - Dazu zählt jedenfalls das Einspielen der jeweils aktuellen Sicherheitsupdates und eine Kontrolle über die installierten Anwendungen sowie über den Zugriff auf diese Geräte.
    - Zum Schutz vor unbefugter Nutzung der Komponenten sind zudem je nach eingesetztem Gerät, folgende Maßnahmen erforderlich: Vollständiges Schließen des Webbrowsers oder Sperre des Geräts (Bildschirmsperre).
- 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
    - 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[3]. 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)

[3] 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@$$w0rd' 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 Widerrufskennworts (dieses wurde in der Regel während der Registrierung festgelegt) und/oder anhand eines persönlichen Widerruf-Codes (zum Beispiel anhand des Registrierungscodes bei Registrierungen über das primesign OnBoarding Service) erwirkt werden. Ein Widerruf kann auch eine erneute Legitimation erfordern. Aus Sicherheitsgründen wird im Ermessensfall einem Widerrufsantrag 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 (Virusschutz, 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
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